NORTH ATLANTIC TREATY
ORGANISATION

RESEARCH AND TECHNOLOGY
ORGANISATION

AC/323(IST-035)TP/32

www.rta.nato.int

RTO TECHNICAL REPORT **TR-IST-035**

Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies

(Sensibilisation à l’émergence des technologies sans fil : Technologies émergeantes et normes de réseaux personnels et ad-hoc)

This Technical Report represents the Final Report of IST-035/RTG-015 submitted by the members of IST-035/RTG-015 for the RTO Information Systems Technology Panel (IST).

Published April 2007

NATO HQ - QG OTAN
DMS 1579737
DOCUMENT

Distribution and Availability on Back Cover

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **01 APR 2007**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies (U)**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Research and Technology Organisation North Atlantic Treaty Organisation BP 25, F-92201 Neuilly-sur-Seine Cedex, France**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
See the report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified - NATO	**unclassified**	**unclassified**	**UU**	**122**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

NORTH ATLANTIC TREATY
ORGANISATION

RESEARCH AND TECHNOLOGY
ORGANISATION

AC/323(IST-035)TP/32

www.rta.nato.int

RTO TECHNICAL REPORT **TR-IST-035**

Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies

(Sensibilisation à l’émergence des technologies sans fil :
Technologies émergeantes et normes de
réseaux personnels et ad-hoc)

This Technical Report represents the Final Report of IST-035/RTG-015 submitted by the members of IST-035/RTG-015 for the RTO Information Systems Technology Panel (IST).

Prof. George Stassinopoulos (Greece), Editor

Contributions in national alphabetical order:
L. Boucher (CA), M. Churavy (CZ), T. Plesse (FR), D. Marquart (GE),
G. Stassinopoulos (GR, Chair IST-035), S. Kyriazakos (GR),
N. Papaoulakis (GR), D. Nikitopoulos (GR), T. Maseng (NO)

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote co-operative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective co-ordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also co-ordinates RTO's co-operation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of co-operation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier co-operation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

The content of this publication has been reproduced
directly from material supplied by RTO or the authors.

Published April 2007

Copyright © RTO/NATO 2007
All Rights Reserved

ISBN 978-92-837-0052-4

Single copies of this publication or of a part of it may be made for individual use only. The approval of the RTA Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

List of Figures

List of Tables

Glossary

AAS	Advanced Antenna System
ACK	ACKnowledgement
AMRIS	Ad-hoc Multicast Routing protocol utilizing Increasing id numberS
AODV	Ad-hoc On-demand Distance Vector (MANET routing protocol)
ARQ	Automatic Repeat reQuest
ATM	Asynchronous Transfer Mode
BE	Best Effort
BPSK	Binary Phase Shift Keying
BRAN	Broadband Radio Access Networks
BS	Base Station
BWA	Broadband wireless access
C3I	Command, Control, Communications & Information
CBC	Cypher block chaining
CBR	Constant bit-rate
CBRP	Cluster Based Routing Protocol (MANET routing protocol)
CEDAR	Core Extraction Distributed Ad-hoc Routing (MANET routing protocol)
CID	Connection ID
COTS	Commercial Off The Shelf
DF	Direction finding
DFS	Dynamic frequency selection
DREAM	Distance Effect Algorithm for Mobility
DSDV	Destination Sequenced Distance Vector routing
DSR	Dynamic Source Routing
DSRP	Dynamic Source Routing Protocol (MANET routing protocol)
EMCON	EMission CONtrol
ESSID	Extended service set identifier
ETSI	European Telecommunications Standards Institute
EW	Electronic Warfare
FDD	Frequency-division duplex
FSR	Fisheye State Routing
HSR	Hierarchical State Routing
IARP	IntrAzone Routing Protocol
ICMP	Internet Control Message Protocol
IEEE	Institut of Electrical and Electronic Engineers
IERP	IntErzone Routing Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
INRIA	Institut National de la Recherche en Informatique et Automatique
IP	Internet Protocol (now v4, in future v6)
IST	Information Systems Technology

LMDS	Local Multipoint Distribution Service
LOS	Line of sight
LPD	Low probability of detection
MAA	MANET Authentification Architecture
MAC	Medium Access Control
MAC	Medium access control layer
MANET	Mobile Ad-hoc NETwork
MMDS	Multichannel Multipoint Distribution System
MPR	Multi Point Relay node
NC3O	NATO Consultation Command & Control Organization
NRL	Navy Research Laboratory
nrtPS	Non-real-time Polling Services
OFDM	Orthogonal frequency division multiplex
OFDMA	Orthogonal frequency division multiple access
OLSR	Optimized Link State Routing (MANET routing protocol)
OSPF	Open Shortest Path First (Internet routing protocol)
PAN	Personnal Area Network
PAR	Project Authorization Request
PDU	Protocol Data Unit
PHY	Physical layer
PICS	Protocol Implementation Conformance Statement
PKM	Privacy Key Management
QAM	Quadrature Amplitude Modulation
QOS	Quality of Service
QoS	Quality of Service
QPSK	Quadrature Phase Shift(ed) Keying
RDMAR	Relative Distance Microdiscovery Ad-hoc Routing Protocol
RDN	Reliable Delivery Neighbourhood
RID	Routeur IDentifier
RTG	RTO Task Group
RTO	Research & Technology Organization
rtPS	Real-time Polling Services
SC	Single-carrier modulation
SDU	Service Data Unit
SFs	Service flows
SSs	Subscriber Stations
TBRPF	Topology Broadcast based on Reverse Path Forwarding (MANET routing protocol)
TC	Topology Control
TCP	Transfer Control Protocol (TCP/IP)
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time-division duplex
TDMA	Time Division Multiple Access
TORA	Temporally Ordered Routing Algorithm (MANET routing protocol)
TTL	Time To Live

UDP	User Data Protocol (UDP/IP)
UGS	Unsolicited Grant Services
UHF	Ultra High Frequency radio (300 – 3000 MHz)
VHF	Very High Frequency radio (30 – 300 MHz)
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WG	Working Group
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networks
WPAN	Wireless Personal Area Network
ZR	Zone Radius
ZRP	Zone Routing Protocol (MANET routing protocol)

Information Systems Technology Panel

CHAIRMAN

Prof. Ann MILLER
Distinguished Professor of Electrical and
Computer Engineering
University of Missouri-Rolla
125, Emerson Electric Co. Hall
Rolla, MO 65409-0040
UNITED STATES

DEPUTY CHAIRMAN

Prof. Marek AMANOWICZ
Ministry of Defence
Military Communications Institute
05-130 Zegrze
POLAND

IST-035 TASK GROUP CHAIRMAN

Prof. George STASSINOPOULOS
National Technical University of Athens
GREECE
E-mail: stassin@cs.ntua.gr

PANEL EXECUTIVE

From Europe:

RTA-OTAN
Lt.Col. P. PRODHOME, FAF
IST Panel Executive
7 rue Ancelle, BP 25
F-92201 Neuilly-sur-Seine Cedex
FRANCE

From the USA or CANADA:

RTA-NATO
Attention: IST Executive
PSC 116
APO AE 09777

Tel: +33 (1) 5561 2280 / 82 – Fax: +33 (1) 5561 2298 / 99 – E-mail: prodhomep@rta.nato.int

Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies

(RTO-TR-IST-035)

Executive Summary

How wireless technologies and devices are proliferating finding wide acceptance and possibilities for deployment is the key target of this report.

Range, bandwidth and power constraints are, as in the civilian world, prominent issues and each technology described is placed for covering part of these conflicting requirements.

The report starts with ad-hoc networking concepts and maturing technological solutions. Ad-hoc networking is a necessary companion to wireless communication, due to the inherent lack of reliability of any wireless based link level protocol. It is particularly important in the military case, where flexible deployment, need for reconfiguration and adaptation to changing scenarios and situations bring ad-hoc requirements up to the application level.

The pertinent wireless technologies of the 802.11 families are then described one by one in their physical, medium access and link layer aspects. Point to point, point to multipoint and fully symmetric arrangements listed against range (tens of meters up to several kilometers) and offered bandwidth call for the examination of the 802.16 series of standards. For ranges in the order of meters, special technologies apply discussed under the heading of PANs (Personal Area Networks). These technologies, with emphasis on low power, have to be seen also in the context of a wider range of terminals (‘sensors’, personal weapons, low end and possibly throw away devices) supplementing the traditional needs of data and voice communications. Comparative tables are used to summarize key characteristics and to demarcate the ranges of possible usage for each technology. Moreover the interplay of the described technologies is summarized under the common framework of the so-called “Book of Visions”, which loosely describes interworking scenarios in a wider application centric context.

Attention is drawn to security issues for each particular technology giving the present (usually unsatisfactory status) and possible ways to ensure characteristics more acceptable for military applications. Testing and verification methodologies are also upcoming and relevant possibilities are overviewed.

To each major technological area (ad-hoc networking, wireless communication standards) ongoing military experiments and developments are also included. These are current activities of the nations contributing to this report. This shows, on one hand, the desirability of COTS usage, and on the other, the need to properly cover military requirements. The optimal trade-offs found for civilian applications cannot always coincide with those for a military design; however examples on how to choose the best from the two worlds are shown.

System interceptability and ECM issues are then overviewed, collecting several relevant points from the previous chapters and examining this very important aspect in a self contained fashion. The report then concentrates on requirements drawn from internal NATO documents in an effort to summarize and conclude on the military prospects of emerging wireless technologies as well as to key open problems, which call for their solution as a condition to military deployment.

Sensibilisation à l'émergence des technologies sans fil : Technologies émergeantes et normes de réseaux personnels et ad-hoc

(RTO-TR-IST-035)

Synthèse

La manière dont les technologies et les dispositifs sans fil se développent et sont de mieux en mieux acceptés et leurs possibilités de déploiement sont l'objectif clé de ce rapport.

Les contraintes de la portée, de la bande passante et de l'alimentation sont, dans le monde civil, des questions majeures et chaque technologie décrite couvre une partie de ces exigences conflictuelles.

Le rapport commence par des concepts de mise en réseau ad-hoc et des solutions technologiques de maturité. La mise en réseau ad-hoc va nécessairement de pair avec la communication sans fil, en raison du manque inhérent de fiabilité de tout protocole de niveau de liaison sans fil. Cela est particulièrement important, dans le contexte militaire, où le déploiement flexible, le besoin de reconfiguration et d'adaptation aux situations et aux scénarios modifiés conduisent les exigences ad-hoc au niveau d'application.

Les technologies sans fil appropriées des familles 802.11 sont ensuite décrites, les unes après les autres, selon leurs aspects physiques, d'accès au support et de couche de liaison. Les arrangements complètement symétriques, point à point et multipoints répertoriés par rapport à la portée (de dizaines de mètres à plusieurs kilomètres) et la bande passante offerte exigent l'examen des séries de normes 802.16. Pour les portées de l'ordre des mètres, des technologies spéciales s'appliquent sous la rubrique PAN (réseaux personnels). Ces technologies, avec un accent sur une faible alimentation, doivent être également vues dans le contexte d'une gamme plus large de terminaux (« capteurs », armes personnelles, dispositifs bas de gamme et éventuellement à usage unique) supplémentant les besoins traditionnels des communications vocales et de données. Des tableaux comparatifs sont utilisés pour résumer les caractéristiques clés et démarquer les champs d'utilisation possibles pour chaque technologie. De plus, l'interaction des technologies décrites est résumée sous le cadre commun du dénommé « Livre des visions », qui décrit plus ou moins les scénarios d'interfonctionnement dans un contexte centré d'application plus large.

L'attention est appelée sur les questions de sécurité pour chaque technologie particulière donnant les façons actuelles (généralement à statut insatisfaisant) et possibles de garantir des caractéristiques plus acceptables pour les applications militaires. Les méthodologies d'essai et de vérification sont également à venir et les possibilités pertinentes sont présentées brièvement.

Pour chaque domaine technologique majeur (mise en réseau ad-hoc, normes de communication sans fil), les expériences et les développements militaires en cours sont également inclus. Il s'agit des activités actuelles des pays participant à ce rapport. Cela montre, d'une part, le souhait de l'utilisation des COTS, et, d'autre part, le besoin de couvrir correctement les exigences militaires. Les compromis optimums trouvés pour les applications civiles ne peuvent pas toujours coïncider avec ceux destinés aux applications militaires ; cependant, des exemples sur la manière de choisir ce qui est le mieux dans les deux mondes sont indiqués.

La capacité d’interception du système et les questions sur les CME sont souvent passées en revue, regroupant plusieurs points pertinents, à partir des chapitres précédents et examinant cet aspect très important de manière séparée. Le rapport se concentre ensuite sur les exigences tirées des documents internes de l’OTAN dans le souci de résumer et de conclure sur les perspectives militaires des technologies sans fil naissantes ainsi que sur les problèmes clés ouverts, dont la solution est une condition du déploiement militaire.

Chapter 1 – INTRODUCTION

The context of IST-035/RTG-015 work is centered on a broad categorization of technologies and military application areas, as shown in the following table:

Table 1-1: Context of IST-035/RTG-015 Work

WirelessLAN (10m - 1km) • 802.11 a,b,h,e,i • 802.16	Ad-hoc NETwork	Command Post & vehicles	Military Relevance + Interoperability + Urban issues
WirelessPAN (<10m) • 802.15 •Bluetooth •UWB		Soldier Network	

The present document presents for each technology architecture, security, QoS, performance and frequency aspects. As a reference document it not only discusses technology, but also positions it in the context of the relevant operational deployment. For that reason, the document will be able to take as a starting point the classification of the operational use of COTS systems, made by the SCI-107 WG.

This document is structured around 9 chapters. Chapter 1 is the introduction that presents the layout of this document. Chapter 2 refers to ad-hoc networks focusing on MANET. Chapter 3 is an overview of WLAN technologies, while in Chapter 4 broadband wireless access technologies and protocols are presented. Chapter 5 is a general approach of a Personal Area Network. Command post and urban operation are presented in Chapter 6, while in the next chapter the soldier network is described. Security, ECM and ESM issues are handled in Chapter 8 and finally we sum up with the conclusions in Chapter 9, in the form of comments on how to cover specific NATO requirements. In addition there are annexes at the end of the document that give more technical information about the topics resented in this document.

Chapter 2 – AD-HOC NETWORKING

2.1 MANET OPERATIONAL EMPLOYMENT

MANET protocols can be implemented on various radio subnetworks: "classical" military VHF/UHF networks, militarized WLAN.

The need for Wireless LAN has been identified at the Brigade, Battalion and Platoon levels. In the future, wireless LAN could also be used inside a group of mobile entities relatively closed one from the others, such as in a tank squadron on the move.

The mobile ad-hoc network is especially useful in rapid deployment. Military teams require fast, effective communications when they rush to an operational scenario.

MANET networks has to meet C3I system requirements, according to the NATO definition. On a C3I tactical level, MANET network has to gather information about enemy and own forces and the environment in which they are deployed, disseminate orders to execute decisions, acquire reports from lower level units.

MANET Protocols has to solve the main problems due to tactical behavior:

- Range of the radio networks: a mobile or a group of mobile may be temporarily isolated from a network (for many reasons including distance and relief): relaying capacities, back-up networks and reconfiguration are important functions to keep a maximum connectivity with acceptable data rate and quality of service;
- Moves of users from one network to another or from on access interface to another that need adaptation of the routing and may be of the addressing;
- Moves of assets and LANs (Aircraft, Navy ships) that may imply other routing functions; and
- EMCON communication restrictions: When a mobile platform, due to operational security, is operating under EMCON directives it can't be capable of transmitting any information and it is unable to respond any received signals. Therefore co-operative communications are not possible; tactical units are committed solely to a "receive only" communication network or unidirectional link. Solutions to the EMCON communication restrictions can be envisaged at different level and require both doctrinal aspects as well as protocol implications.

2.2 MANET ROUTING

2.2.1 Overview

Mobile ad-hoc networking is to extend mobility ("Mobile IP" technology is to support a mobile host connected through various means to the Internet other than its well-known fixed-address domain space), into the field of autonomous, mobile, wireless domains, where a set of nodes, which may be routers and hosts, themselves form the network routing infrastructure in an ad-hoc mode.

MANET concerns with the autonomous system of mobile routers, connectedly wireless links.

Because of the different nature of wireless networks as compared to the fixed wired networks, the existing solutions are not suitable for this environment. This situation opens a wide variety of issues and challenges the designers of routing protocols with a complex combination of conflicting problems. The main challenges include the dynamic and rapidly changing topology, low available bandwidth, lack of a centralised entity, large network diameters, existence of unidirectional links, scaling up problems, and the security considerations for these shared medium access networks.

In an encumbered mobile network, to quickly discover the various options of routing, is preferable to calculate the single shortest road.

These issues require that a routing protocol for a mobile ad-hoc network should be self starting and self organising, which provides the multi-hop, loop free paths to the required destinations in the network. Because of the mobility of the nodes, there should be a mechanism of dynamic topology maintenance, and rapid convergence of the protocol should be assured to stabilise the system. But the daunting task is to make it all possible using the minimum memory and bandwidth resources, and minimal overhead for data transmission. It is also required from these protocols to be scaleable to large networks.

In IETF WG, MANET is now focus on unicast and broadcast issues, but no more on multicast.

2.2.2 Concepts Developed by MANET

Architectural and protocol issues are here discussed.

2.2.2.1 Hierarchy of MANET Routing Protocols

MANET routing protocols work at the Network Layer level. The general MANET architecture is shown in Figure 2-1 below:

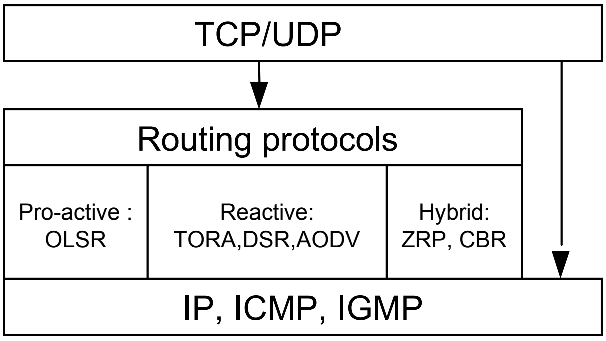


Figure 2-1: Hierarchy of MANET Routing Protocols.

Some functionalities done by different routing protocols individually are:

- **Encapsulation**. To improve the overall network performance, several control messages are encapsulated and aggregated into a single packet. In this way, it reduces the “number” of control messages to send, which, in consequence, reduces the “attempts” for the channel access. So the per-message, multiple access “delay” in contention based schemes is reduced.
- **Network Level Address Resolution**. There’s packets to map RIDs to IP addresses, which is similar to MAC address to IP address mapping. RIDs (Router IDs) provide the possibility to have more than one physical interface associated to a router.
- **Link Status Sensing**. There’s mechanism of exchange of BEACON and ECHO packets between neighbours for the neighbourhood detection. Data and ACK packets are also considered as the BEACON and ECHO equivalent packets, to reduce control traffic during data transmission.
- **One-Hop Broadcast Reliability**: To provide a reliable broadcast between the neighbours, concept of Colour and Sequence Number associated to the reliable delivery neighbourhood (RDN) can be used. When a node receives a packet with correct Colour and Sequence Number, it

acknowledges the packet. There is also a Point to multi-point selective repeat algorithm for reliable multicast.

- **Security Authentication**. MAA (MANET Authentication Architecture) can provide nodes to choose among the simple to complex authentication options, depending upon their security requirements. MAA uses cryptography requiring distribution/exchange of encryption key information.
- **Multi-Point Relaying**. Multi-point relaying is a technique which attempts to minimise the duplicate re-transmissions of the broadcast packets in the same region. For the flooding of the packets in the networks, MPR technique efficiently forms a spanning tree to diffuse the packet in the whole network, using minimum re-transmissions. The concept behind is, that instead of every router, only selective routers (called the multi-point relays of a node) re-transmit the packet, still covering the same area.

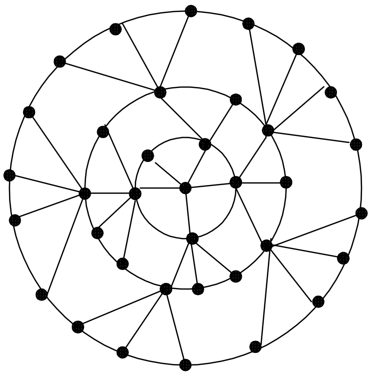


Figure 2-2: MPR Tree.

MANET has also developed a classification for the proposed routing protocols.

2.2.2.2 Classification of Routing Protocols

Several routing protocols for the mobile ad-hoc networks are presented in the MANET working group. These protocols can be mainly categorise into three types:

- Proactive,
- Reactive, and
- Hybrid.

2.2.2.3 Proactive Protocols

These protocols use an adaptive system of routing, based on the exchange of control packets. The connectivity among the neighbors is managed by periodically sending the HELLO type messages to keep the links alive. Furthermore, all the network nodes participate in exchanging the topology information, and continuously update the reachability information in the nodes routing tables. In this way, the route is immediately available when requested. The disadvantage of this scheme is that it consumes substantial bandwidth for control traffic and exchange of information, which may never be required.

So proactive protocols are effective when a high percentage of network nodes are source of traffic. Proactive protocols behave rather similar to traditional IP routing protocols; this brings better compatibility with the transport protocols and Internet applications.

2.2.2.4 Reactive Protocols

The reactive routing protocols work passively and do not take initiative for finding a route which is not required. They attempt to discover route only "on demand" by flooding their Query packet. The data packet is put on wait, until the route is found, indicated by the reception of a reply packet from the destination (or from a node having the route to the destination). In this way, resources are not consumed for sending information, which is not required, and once a route is known, bandwidth is consumed mostly for data transmission.

The disadvantage of this technique is that enormous bandwidth is consumed for the global search (flooding) and there are large delays in sending the data packets.

So reactive protocols are effective when a small percentage of network nodes are source of traffic and when network topology is very dynamic.

2.2.2.5 Hybrid Protocols

The hybrid routing protocols adopt a mixture of proactive and reactive schemes or a derivative of one, by optimizing either of the two routing techniques. Mostly the currently proposed protocols in MANET group the nodes in zones or clusters to form a sort of hierarchical routing. The routing protocol used inside the zone or cluster is different from the protocol used to find the routes for the destinations outside the zone or cluster. The suitability of these type of protocols greatly depends upon the network requirements and conditions, and hence it is seen that it is difficult to specify the application domain of the hybrid protocols, and therefore any optimization done is also arbitrarily dispersed.

2.2.3 Examples of Existing Protocols

Several protocols are discussed below in some detail.

2.2.3.1 Reactive Protocols

2.2.3.1.1 Temporally Ordered Routing Algorithm (TORA) – NRL / Washington

TORA is a reactive protocol in the MANET framework [2]. Its aim is to minimize the control traffic overhead for routing. Therefore, it provides minimal routing functionality, which gives multiple, loop free routes, which may not necessarily be the optimal routes. It also tries to establish routes as quickly as possible. To help reducing the control traffic, it minimizes the algorithmic reactions to the topological changes by reacting only when necessary and does not respond to all link changes. It also tries to localize the effect of a link change.

The protocol is best suited for very large networks, with a limited bandwidth. Because of its reactive nature, it generates a huge amount of flooding in search of a route. This makes it unsuitable for the real time, delay-constrained traffic. It tolerates the mobility of the nodes causing link breakage, without generating any control traffic, as long as this mobility does not affect the currently active routes.

The functioning of TORA is based on flooding the Query packet when a route is needed for a destination. This flooding of the Query packet is replied with an Update packet by a node, which is a neighbor of the destination node. While the Update packet passes through the network to arrive at the source node, each node in the way form a route towards the destination by directioning their links. A concept of "height" of a node is used to determine its downstream and upstream links for a specific destination. The actual data packet is transmitted when the source receives the update packet, and a route is established to the destination.

The maintaining of the routes is done using a “link-reversal” algorithm, when a node no more has a route to a destination because of a link breakage. If a partition is detected in this process, the routes are erased for that destination.

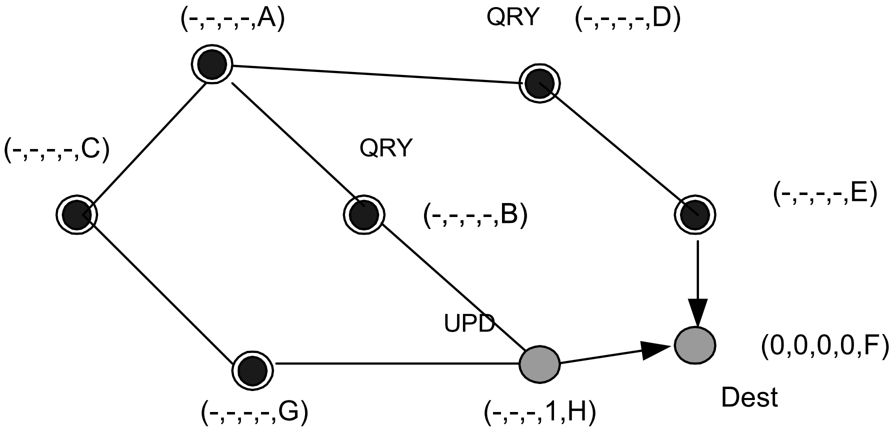


Figure 2-3: An Example of Route Searching in TORA.

2.2.3.1.2 Dynamic Source Routing (DSR) – Dave Johnson / Carnegy Melon

DSR is another reactive protocol presented in the MANET working group [3]. The protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad-hoc network. No periodic messaging is required, and no reaction to unconcerned changes in the topology is shown. The protocol uses the source routing; the complete route is put by the source node in each data packet sent. The advantage of source routing is that the intermediate nodes in the route do not need to maintain any routing information, to forward the packets to the destination. As there are no periodic router advertisements and link status packets, the overhead of DSR is greatly reduced when the network topology is quite stable, where the protocol uses most of the bandwidth for data transmission.

The functioning of DSR is based on flooding the Route Request packet when a route is required for a destination. While this Route Request packet propagates in the network, each node puts its address in the packet header. When this packet reaches the destination (or a node having route to the destination), a Route Reply packet is sent to the source node by inverting the route contained in the Route Request packet. The source then uses this route in each data packet header, it sends.

2.2.3.1.3 Ad-hoc On-Demand Distance Vector (AODV) – C. Perkins / NOKIA / Project RoofTop

AODV provides quick, loop free convergence [4]. It uses the Distance Vector algorithm by introducing a new concept of “Destination Sequence Number” to avoid the problems associated with the Distance Vector algorithm. It has triggered updates and tries to minimize the latency for the route replies, which is a characteristic of the reactive protocols.

The functioning of AODV is also based on flooding the Route Request packet in search of route for a destination. While this Route Request packet propagates in the network, a reverse route to the source is established along the way. When this packet reaches the destination (or a node having route to the destination), a Route Reply packet is sent, in unicast, to the source node using this reverse path.

The maintenance of routes is done only for the active routes. AODV also has its multicast routing protocol.

2.2.3.1.4 Pro-Active Protocol

Proactive protocols are here discussed.

2.2.3.1.4.1 Optimised Link State Routing Protocol (OLSR) – Paul Muhlethaler / INRIA

OLSR is a pro-active protocol to support the large, dense mobile networks, with high nodal mobility and topological changes [5]. The protocol is based on the link state algorithm, and hence inherits the stability of the algorithm. It uses the concept of multi-point relays to calculate the route towards any destination in the network. The multi-point relays provide the optimal routes, and due the pro-active nature of the protocol, these routes are immediately available, when needed.

The protocol is best suited for the dense networks, where lot of traffic is going on between different [source, destination] pairs at different times. The change in [source, destination] pair does not generate any extra control traffic, and so the overhead of control traffic is independent of the data traffic pattern (contrary to the reactive protocols).

The functioning of the OLSR protocol is based on periodically diffusing a topology control packet in the network. The volume of this control information is optimized to exchange MPRs (multi-point relays) of a node, instead of all its neighbors. The flooding of these control messages is optimized by using MPR forwarding and hence saves a significant amount of bandwidth in dense networks, by efficiently and selectively re-transmitting the messages. The protocol adapts rapidly to the topological changes, by increasing the frequency of TC packet, when a change in its MPR set is detected. The protocol manages a topology table to gather the network information obtained from the TC packets, and on the basis of this table, it calculates its routing table.

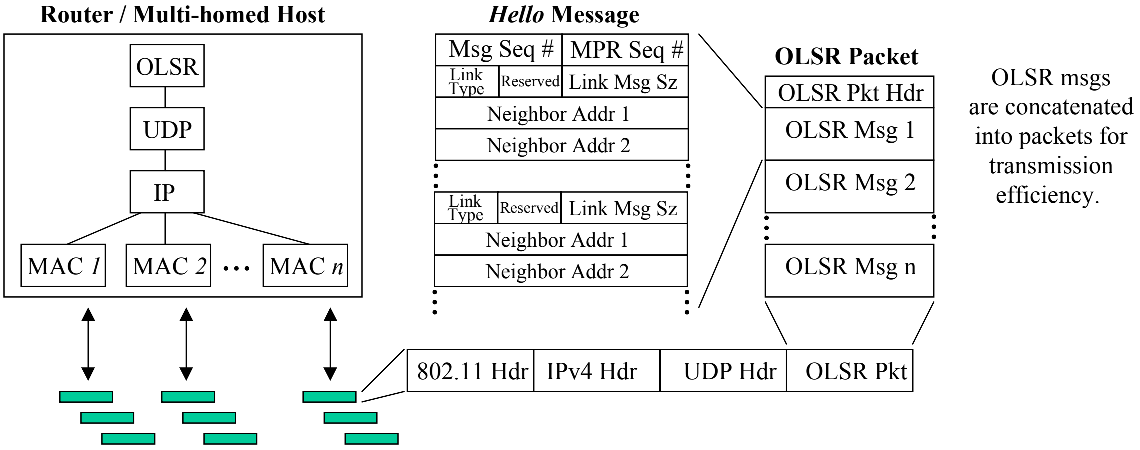


Figure 2-4: OLSR Protocol.

OLSR packets are UDP type and are emitted via port 698. Each frame is made up of the following fields:

- Frame length (in bytes) which is the PDU size;
- Sequence number;
- Type of message, number between 0 and 127 which identifies the information type;
- Message length (in bytes) which is the SDU size;
- Source address;

- TTL (Time to Live), meter which is decremented of 1 with each bound (when TTL=0, diffusion of the frame is stopped);
- Hop count, meter which is incremented of 1 with each bound; and
- Message (payload).

2.2.3.1.5 *Topology Broadcast based on Reverse-Path Forwarding (TBRPF) – Richard Ogier / Stanford Research Institute*

TBRPF is a proactive, link-state routing protocol designed for mobile ad-hoc networks, which provides hop by hop routing along minimum hop paths to each destination. Each node running TBRPF computes a source tree (providing paths to all reachable nodes) based on partial topology information stored in its topology table, using a modification of Dijkstra's algorithm. To minimize overhead, each node reports only part of its source tree to neighbors. This is in contrast to other protocols in which each node reports its entire source tree to neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reportable part of its source tree. Each node also has the option to report additional topology information (up to the fill topology), to provide improved robustness in highly mobile networks. TBRPF performs neighbor discovery using « differential » HELLO messages which report only changes in the status of neighbors. This results in HELLO messages that are much smaller than those of other link state routing protocols.

2.2.3.1.5.1 Hybrid Protocols

Next we discuss Hybrid protocols, where one attempts to combine the best properties of the proactive and reactive ones.

2.2.3.1.5.2 Hierarchical Routing for Large Networks

The case of large networks in handled first.

Large multi-hop shared channel radio networks have the problem of a reduced available bandwidth. As the number of network nodes increases, the available bandwidth per node decreases, making the already scarcely available bandwidth a precious resource. Proactive protocols tend to reduce the performance in very large networks by constantly consuming an important part of bandwidth for the link state updates. The reactive protocols, on the other hand, works well as long as there is no link change, but they paralyze the whole network for sometime by their Query flooding in search of a route. Hierarchical routing may be a better option in these large networks. The nodes of the network are grouped into clusters, which are grouped into superclusters, and so on.

Hierarchical routing is employed in variety of ways. Generally, the hierarchical routing protocols hide the details of faraway parts of the network from the nodes. In some implementations, the information about faraway parts of the network may be transmitted less frequently, while the local information is send more rapidly. Yet another form of hierarchical routing involves sending information to the nodes that need it.

The main issues in the hierarchical algorithms requires a description of how the clusters or superclusters are formed, how the cluster membership is advertised, how the routes are computed, and once the routes are established, how the data packets are forwarded.

2.2.3.1.5.3 Zone Routing Protocol (ZRP)

ZRP is hierarchical routing protocol presented in the MANET working group [6]. It is suitable for a wide variety of mobile ad-hoc networks, especially those with large network spans and diverse mobility patterns. It has an adaptive behavior to set its functioning according to the actual network requirements. It uses a proactive scheme to build routes in its zone (with the radius of x hops), and applies a reactive scheme to find routes outside of its zone (more than x hops away).

A Zone Radius, in number of hops, is defined for the network, taking into account the network mobility, rate of topological changes and the traffic conditions. Then the Routing Zone is defined for each node, and includes the nodes whose minimum distance is less than or equal to the zone radius. Nodes whose distance is exactly equal to the zone radius are called the Peripheral Nodes. IARP (IntrAzone Routing Protocol) provides routes to destinations within the zone radius. IARP works in a pro-active manner and has the up to date routing information for its zone. When a destination node is not found in the zone, a route request message is “bordercasted” to the Peripheral nodes. Bordercasting is an operation of sending a query to all or some of its Peripheral nodes. To search the route, the peripheral nodes use IERP (IntErzone Routing Protocol), which provides routes to destinations outside the source’s routing zone. IERP uses “bordercasting” at each instance, to search the routes, on-demand.

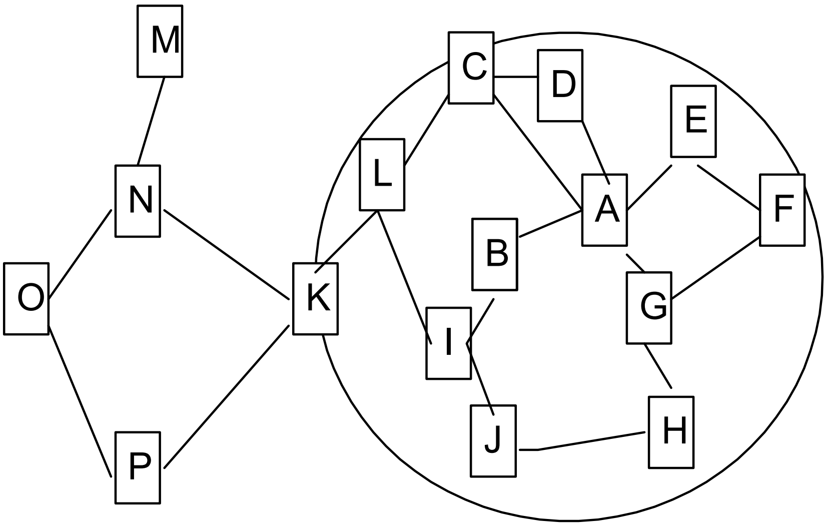


Figure 2-5: ZRP Functioning.

ZRP can be configured for a particular network by proper selection of a single parameter, the routing zone radius.

2.2.3.1.5.4 Cluster Based Routing Protocol (CBRP)

CBRP is a hybrid protocol, using 2-level hierarchical routing [7]. The nodes of the network dynamically group themselves into clusters, by selecting a cluster head. The cluster head has a complete information of the cluster topology, which it transmits to each cluster member. The clusters are joined with the “Gateway” nodes, common to the adjacent clusters. Cluster head knows inter-cluster link state topology through the gateway nodes.

CBRP discovers routes on-demand, with less flooding traffic as the Query is passed only through the cluster heads and the Gateway nodes. When a route is established, the cluster heads can optimize it afterwards, using their topology information, by creating the route between the nodes without passing through the cluster head. CBRP is suitable for middle to large networks with slow node movements, so as to stabilize in finite time with cluster formation.

2.3 CONCLUSION

Clearly mobile radio routing is in the scope of military network applications. More precisely it seems that most of related applications must concern communications in operational units at the bottom of the hierarchy like squadrons.

Numerous technical issues concerning “Mobile Radio network” are primarily the result of the scarce bandwidth of radio. That calls for new routing protocols. Now, we only have proprietary solutions to this issue most of them work at the MAC layer. MANET offers the opportunity to develop a standardized solution to this issue based on routing at the IP layer. This can be considered as an alternative to the use of MAC routing proprietary protocols and to the use of existing IP standards such as OSPF, which are not designed for this type of use.

For military use, MANET proactive protocols seem to be better if we consider that among a tactical network, a lot of users set up communications.

MANET reactive protocols seem to be better on low bandwidth subnetworks (i.e. radio networks), if the density of users is low.

2.4 TECHNICAL SPECIFICATIONS OF A FRENCH MANET TESTBED

2.4.1 Introduction

This section contains the technical specifications of the French MANET (Mobile Ad-hoc NETwork)/ OLSR demonstrator implementing the OLSR routing protocol (version 7). It contains descriptions of demonstrator functionalities, of the hardware and software delivered and description of the demonstrator architecture. The version described here has been implemented as a CELAR testbed on end of December 2002.

2.4.2 MANET/OLSR Demonstrator Features

The MANET/demonstrator features PDAs, laptops, OLSR routers, wireless devices, IP packets, and routing, as explained below. A functional overview of MANET demonstrator is described in Figure 2-6 (although laptops are not represented on this figure).

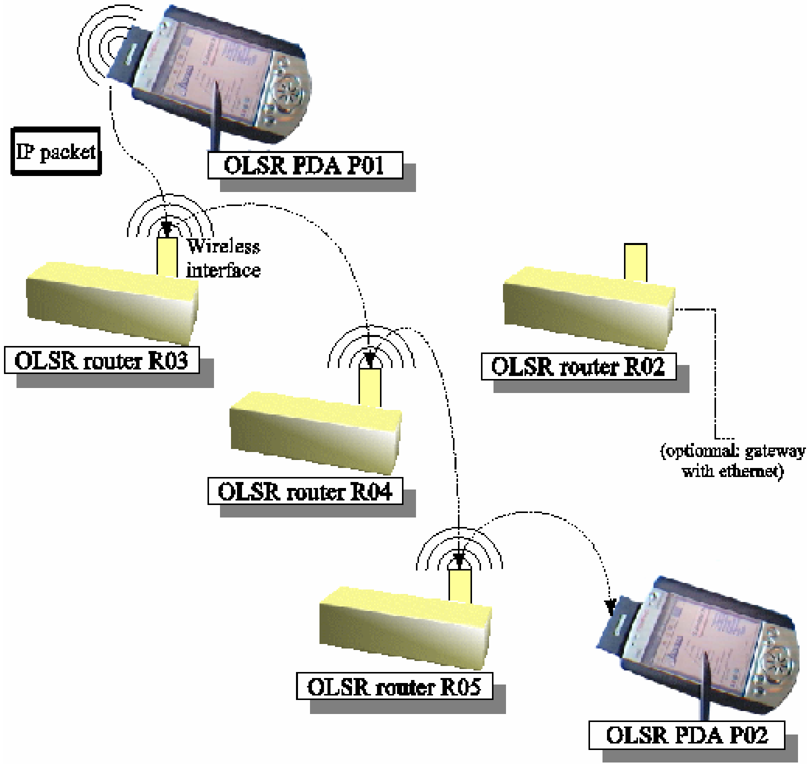


Figure 2-6: MANET/OLSR Demonstrator.

A number of equipments, including standard PDAs, standard laptops, and specific OLSR routers are, each, using wireless networking devices. Those wireless networking devices are used for data transmission using the standard IP protocol, over radio waves. The applications simply use the usual IP networking API. A pre-eminent feature is the ability to perform IP routing, using the wireless routing: that is, when the wireless range is too small for one machine to directly reach another one, an IP packet can, instead, go from machine to machine so that the destination is reached. For instance, on Figure 2-6, the data packet from the PDA P01, would go first to OLSR router R03 by the wireless interface, then will be repeated by R03 to reach router R04, then again from R04 to R05, and finally from R05 to the PDA P02.

The task of setting up IP routing is entirely delegated to the OLSR protocol: using discovery of other machines which are within range, and propagation of that information to the entire network, OLSR is able to set up routes from any machine to any other, provided that at least a path exists (i.e. the network is connected). In addition, OLSR performs this operation dynamically, allowing for low update delays, and hence for mobility. The entity performing the OLSR routing, the OLSR daemon, is central to the demonstrator.

We give an overview of the daemon in the immediately following section ; in the later sections, the demonstrator equipment, which is mostly the environment necessary to run that daemon, is specified. 2.2 OLSR routing. As it was said, the central piece of the demonstrator is the OLSR daemon, which sets up the routing. Figure 2-7 illustrates the inner workings of the OLSR routing.

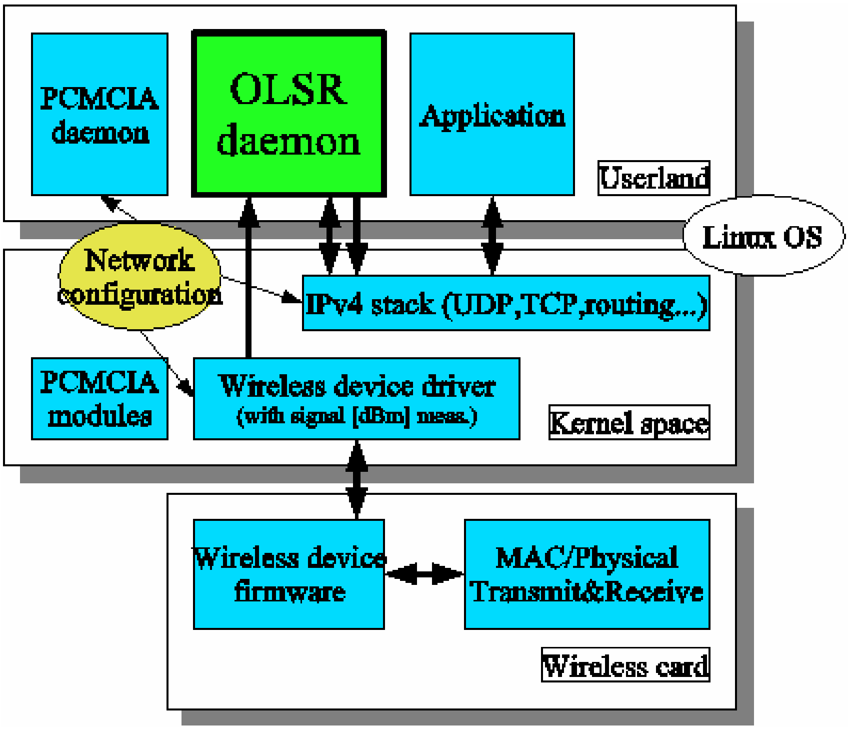


Figure 2-7: OLSR Implementation: The OLSR Daemon.

It is a piece of software running at the application level on the Linux Operating System. This OLSR daemon has three different interactions with the OS:

- It transmits and receives UDP packets (like a standard UDP application), as part of its normal behavior, for discovery of the wireless network topology.
- It configures the IP routes to each discovered destination of the wireless network. The information about the routes is kept in the kernel as part of ``routing table'' of the IP stack. Each "route" is the following information: for a given IP destination address, what is the next hop, that is, the IP address of the machine within range to which we should send the packet 1. On the Figure 2-1, on PDA P01, the next hop for reaching P02 is router R03.
- It can optionally get some meta-information from the driver about UDP packets received: what is the signal/noise with which they were received.

Figure 2-7 shows the main entities involved in the OLSR routing, i.e.:

- The OLSR daemon, implementing a version of the OLSR protocol;
- The kernel which is performing kernel-level tasks, and offers a kernel API;
- An IPv4 stack, part of the kernel, which handles TCP and UDP protocols and encapsulation, IP packet transmission/reception, and IP routing;
- The PCMCIA subsystem, part of the kernel, which allow communication with the wireless device;
- The wireless driver, part of the kernel, which interfaces with the wireless device;
- The wireless device performing MAC/physical transmission; and
- The applications using IP networking, thus implicitly using IP routing.

This results into the following software and hardware requirements:

- Because the OLSR daemon must run on all machines, and it is currently implemented using some Linux kernel API, all machines of the demonstrator are running Linux – including laptop and PDAs. The use of Linux also constrains the hardware.
- Because the PCMCIA configuration scripts, and networking configuration systems are different from one Linux distribution to another, a single fixed distribution is required for each kind of system.
- Because again of inconsistent kernel configuration (routing, ICMP redirection), but also because some low-level improvements are added in the wireless device driver, a fixed kind of driver is required (and shipped).
- Because the wireless device must be supported by the device driver, the choice of those devices is constrained.

2.4.3 Demonstrator Overview

The MANET/OLSR demonstrator includes the following hardware:

Equipment Type	Quantity	System	Linux Distribution
Olsr Router	10	(shipped by INRIA)	(shipped by INRIA)
PDA	4	iPAQ ARM	Distribution Familiar
Laptop	4	Sony VAIO	Distribution Debian 3.0

The demonstrator software includes:

Software	Description	Equipment
OLSR daemon	OLSR protocol version 7	PDA, Laptop, OLSR Router
iperf	Network performance tool	Laptop, OLSR Router
netperf	Network performance tool	Laptop, OLSR Router
Misc. monitoring software	Network performance tool	Laptop

2.4.4 Network Configuration

The IP networking configuration is the following:

Network Type	IP Addresses
Ethernet	10.103.96.0/24
Wireless	10.103.97.0/24

2.4.5 Wireless Network Specification

The wireless radio interfaces used are standard 802.11b interfaces. The technical specifications of the cards are:

Wireless device	PCMCIA, Avaya Wireless PC Card (Silver) (previous versions sold as “Orinoco Silver” and “Lucent Technologies Silver”)
Compatibility	IEEE 802.11b Standard for Wireless LANs (DSSS)
Firmware	Tested with versions 6.04 and 7.52
MAC	CSMA/CA
R-F Frequency Band	2.4 GHz (2400-2500 MHz)
Used sub-channel	Channel 11 (2462 MHz)
Modulation technique	Direct Sequence Spread Spectrum
	CCK (11 and 5.5 Mbps), DQPSK (1 Mbps)
	DBPSK (1 Mbps)
Spreading	11-chip Barker Sequence
Bit Error Rate	Better than 10-5
Nominal Output Power	10 dBm

The reported radio characteristics, range, sensitivity, delay spread are the following:

Data bit rate	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open office	160 m	270 m	400 m	550 m
Semi-open office	50 m	70 m	90 m	115 m
Closed office	25 m	35 m	40 m	50 m
Receiver sensitivity	-83 dBm	-87 dBm	-91 dBm	-94 dBm
Delay spread	65 ns	225 ns	400 ns	500 ns

2.4.6 Ad-hoc Mode

The wireless radio cards are run in a special mode, called the “Ad-Hoc” mode or “Ad-Hoc demo mode”. This mode is not a standard WiFi mode: neither the “infrastructure mode” nor the “Ad-Hoc IBSS” mode. But it is supported on many cards, including the Lucent derivated and the numerous Prism II derivated cards, because it is simply removing all the management/beaconing frames.

2.4.7 Systems Technical Specification

2.4.7.1 OLSR Router Specification

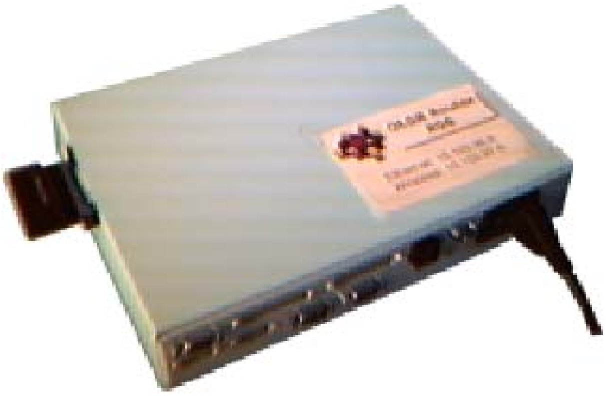


Figure 2-8: OLSR Router.

Here is a summary of the features of the routers:

Hardware	PC mini-motherboard
Processor	486 133 MHz
Memory	16 MBytes
Hard drive	None, 16 MBytes Flash memory instead
Networking	Ethernet NE2000 compatible, 10 Mbps
Wireless Networking	via PCMCIA adapter
System	Linux kernel 2.4.19
	binaries based on Slackware 7.0, 7.1 and 8.0

The OLSR router includes a Linux system, which is a system, based on Slackware 7.0, 7.1 and 8.0, which can be used by direct login (when plugging in a monitor and a keyboard) or via network by telnet.

2.4.7.2 Linux Laptop Specification

The laptop is a VAIO on which Linux is installed. The specifications are as follows:

Hardware	Sony VAIO PCG-C1MHP-FR
Processor	Transmeta Crusoe TM5800 at 867 Mhz
Memory	256 MBytes
Hard drive	30 GBytes
Networking	Ethernet 10/100 Mbps
Wireless Networking	via PCMCIA adapter (or Bluetooth)
System (2*OS)	Windows XP & Linux kernel 2.4.19
	LINUX Distribution Debian 3.0

The following software from the Debian 3.0 distribution is necessary:

Software	Usage
kernel 2.4.19	a recent version of the kernel
pcmcia-cs 3.1.22+	*for PCMCIA adaptor*
orinoco module	for PCMCIA wireless card
wireless-tools (23-2+)	*for wireless card configuration*
xirc2ps	for Xircom Ethernet device
python (2.2)	for scripts and OLSR
minicom	*for communication with iPAQ via serial*
iproute	for advanced routing configuration

2.4.7.3 Linux PDA Specification

The PDA is a iPAQ on which Linux is installed. The specifications are as follows

Hardware	Compaq iPAQ Pocket PC H3950
Processor	Intel PXA 250 at 400 Mhz
Memory	64 Mbytes SDRAM
Hard drive	None, 32 MBytes Flash memory instead
Networking	via PCMCIA adaptor
Wireless Networking	via PCMCIA adaptor
System	Linux kernel 2.4.19
	Familiar v0.6.1
Extension	PCMCIA adaptor
iproute	for advanced routing configuration

The following software from the Familiar v0.6.1 distribution is necessary:

Software	Usage
kernel 2.4.19	a recent version of the kernel
pcmcia-cs	*for PCMCIA adaptor*
orinoco module	for PCMCIA wireless card
wireless-tools (21-1.3+)	*for wireless card configuration*
xirc2ps	for wireless card configuration
python (2.2)	for scripts and OLSR
Complete compilation chain	for recompiling kernel, modules and OLSR
Complete cross-compilation chain	for cross-compiling kernel, and modules

2.4.8 Software

2.4.8.1 Overview

The following software is included:

Software	Description
olsrd and python_olsrd	The basic version of the OLSR daemon and the version with HTTP interface (port 11698)
netperf	Network performance tool
	Client and server (running on default port)
iperf	Network performance tool
route, ifconfig, iwconfig, ...	Standard Linux/Unix tools

- All IP networking applications should work, if they are not using broadcast addresses.
- All standard IP tools should be working, including route, ip, traceroute, ping, telnet.
- The tool netperf is shipped. It allows for TCP and UDP performance measurements.
- The tool iperf is shipped. It allows also for TCP and UDP performance measurements, although with different options, and different result presentation.

2.4.8.2 OLSR

The OLSR daemon shipped is compliant with the version 7 of the OLSR RFC draft (http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-07.txt). It exists in two versions, one with the name olsrd (or std_olsrd), and one with the name python_olsrd. The second might not be available for PDAs; the difference between the two versions is that the second one adds an HTTP interface, which can be used to monitor the status of a given OLSR daemon, as illustrated on Figure 2-9.

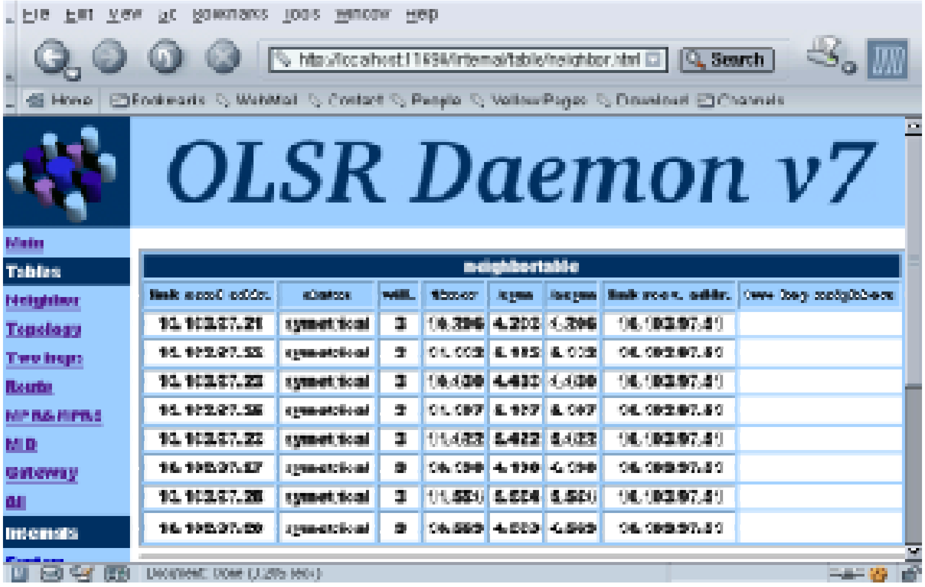


Figure 2-9: A WEB Interface to the OLSR Daemon (python_olsrd).

Version	Draft version 7
Protocol port	1680 (non-standard, standard is 698)
HTTP interface port	11698

2.4.9 References

OLSR page	http://hipercom.inria.fr/olsr/
MANET page	http://www.ietf.org/html.charters/manet-charter.html
Linux kernel	http://www.kernel.org/
Linux PCMCIA system	kernel or http://pcmcia-cs.sourceforge.net/
Linux and wireless devices	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
Debian	http://www.debian.org/
Linux on laptops	http://www.linux-laptop.net/
Linux on VAIO C1MHP	http://this.is.not-mediaways.net/but.i.am/flo/c1mhp/
Linux on PDAs	http://www.handhelds.org/
Linux familiar (iPAQ)	http://familiar.handhelds.org/
`netperf`	http://www.netperf.org/
`iperf`	http://dast.nlanr.net/Projects/Iperf/

2.4.9.1 Demonstrator Architecture (Scenario)

On the figure below, only the 10 INRIA OLSR routers are represented. The 4 mobile PDA terminals and 4 mobile VAIO terminals are not represented.

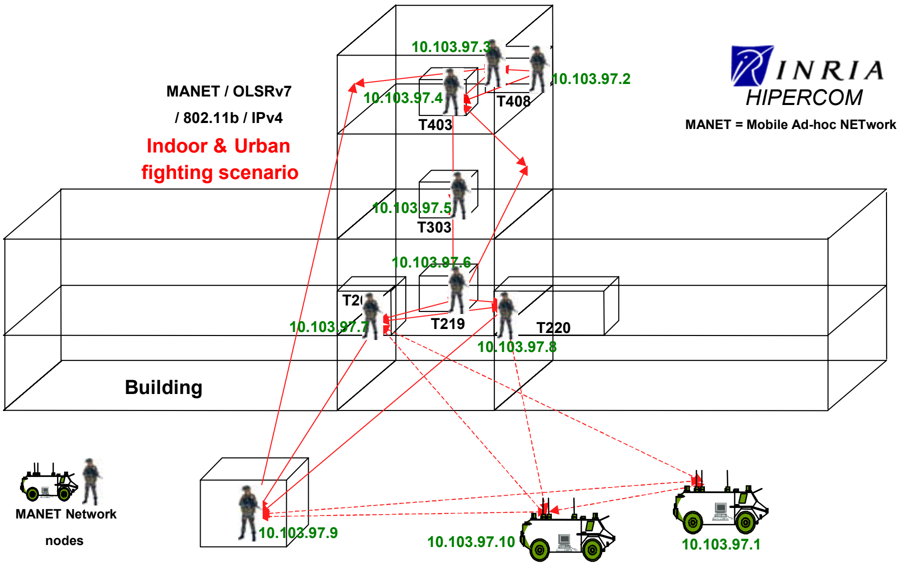


Figure 2-10: Demonstrator Architecture.

In room T408 (level 4), OLSR router (@ 10.103.97.2) is the gateway to INSC wired network.

2.4.9.2 INSC Interconnection Architecture

The figure below shows the interconnection, through FreeBSD router and 6Wind access router, between OLSR CLAN (Coalition LAN) and INSC wired network. The function of FreeBSD router is to set up IPv4/IPv6 tunnels: latest version of OLSR network – version 7, runs with IPv4, and INSC network is IPv6. the 6Wind router is the access router to IPv6 INSC network; it provides security and Quality of Service (QoS).

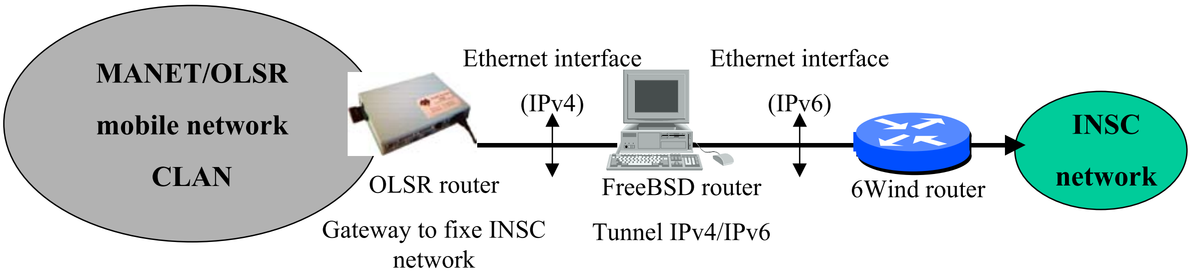


Figure 2-11: INSC Architecture.

2.5 FRENCH PR4G SAP AD-HOC NETWORK

2.5.1 Introduction

This section contains an overview of French PR4G SAP ad-hoc network. PR4G is a French military radio. SAP mode for "Packets Access Service (PAS)". SAP mode is one of modes implemented on the PR4G.

2.5.2 SAP/PAS Network Oriented Mode

PR4G SAP radio (Packet Radio Network) has the following features:

- Slotted Aloha Channel Access;
- Multiple Selective Call;
- Message Transmission (up to 63 kbps);
- Automatic Data Rate Management;
- Mono-Transceiver routing; and
- Up to 59 Pax and 10 relays.

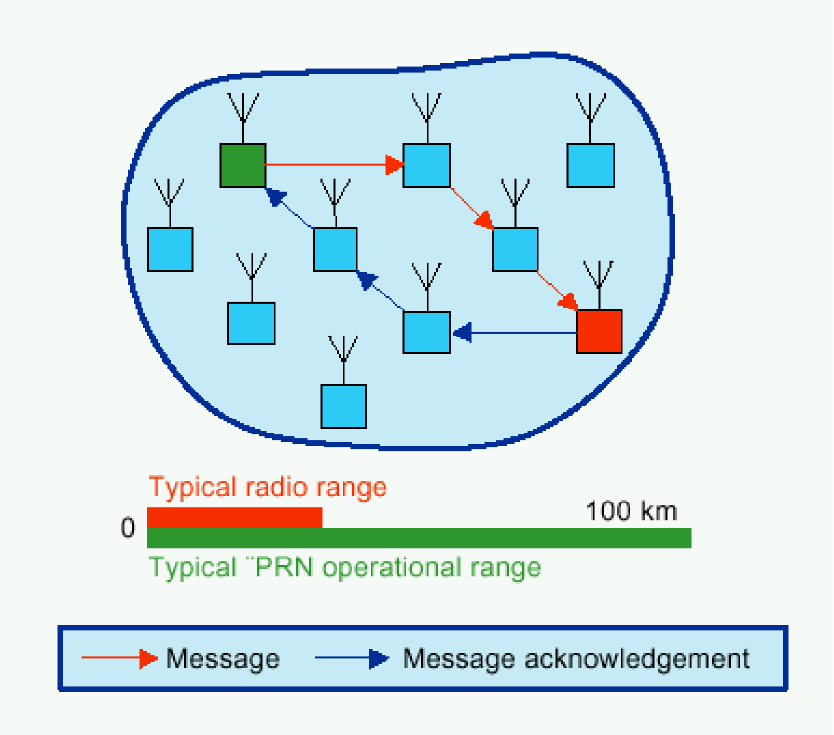


Figure 2-12: SAP/PAS.

Due to its robustness, flexibility and ability to cover large areas, Packet Radio Network technology is seen as the future for non-real time battle-field data transmission, such as Message Handling Systems (Electronic Mail).

2.5.3 Packet Radio Mode

2.5.3.1 Principles

Data communication over extended ranges via automatic routing through different CNR.

2.5.3.2 Advantages

- Fully automatic flood search routing and flow control; and
- Flexible reconfiguration capability.

2.5.3.3 Implementation

- Each subscriber T/R used as a relay station; and
- Application procedures managed externally by computer.

2.5.4 PRNET with PR4G

PRNET is one among the many possible applications using the parameterized general purpose packet data transmission mode embedded in the radio set. The Packet access service inside the radio set has the function of synchronization, coding and interleaving, channel access, packet routing. All real time functions taking advantage of transmitting synchronization and FH facilities.

The PRNET application outside the radio set provides segmentation of message, end to end message acknowledgement and management functions (routing update, flow control, data rate selection).

2.5.5 Packet Radio Application (Routing)

For any destination node, each (relaying) node computes a standard list (neighbor stations in the shortest paths – e.g. “to node z: B or C with 2 hops”), a fallback list (neighbor stations in almost shortest paths – e.g. “to node z: A or D with 3 hops”).

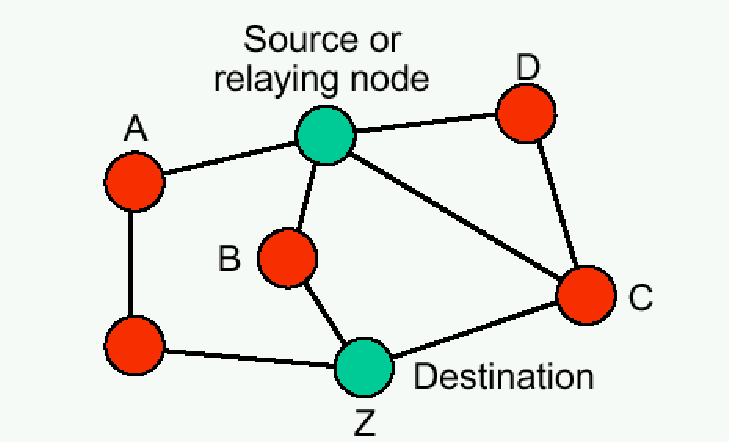


Figure 2-13: Packet Radio Application Routing.

2.5.6 Packet Radio Application Providing Routing Adaptivity

The general idea is depicted through the example below

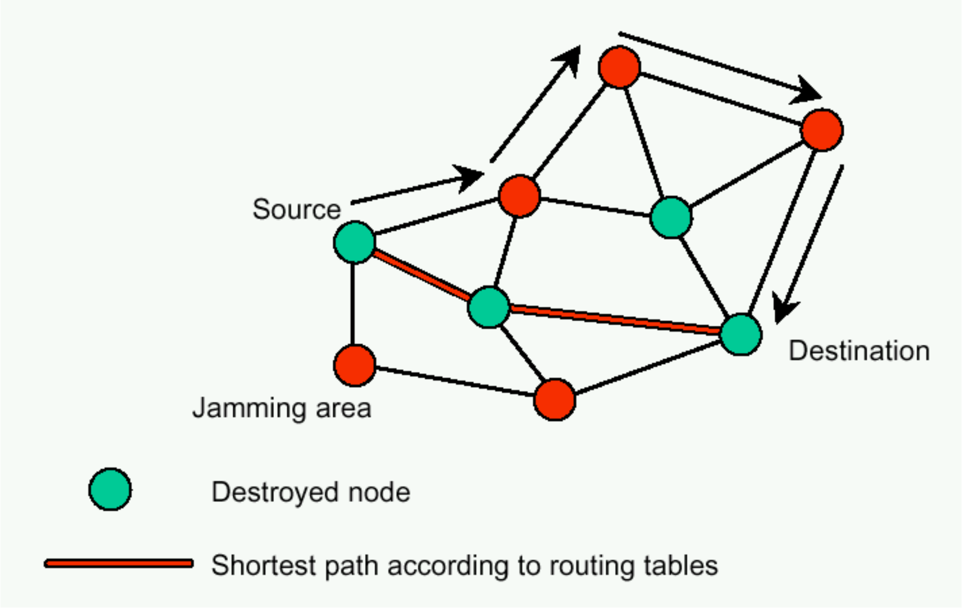


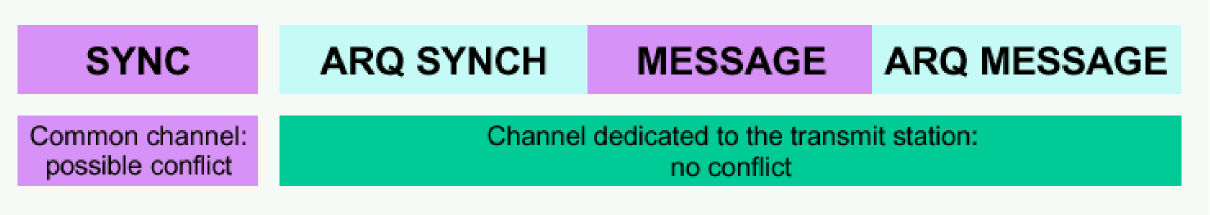
Figure 2-14: Packet Radio Routing.

2.5.7 Synchronization and User Traffic Principles

The channel access slotted based on 100 ms slots (as in TDMA mode). The features of synchronization is the following:

- No master; based on a distributed algorithm;
- Sent in dedicated sync slots; and
- Uses the main hopping channel.

For the User traffic, one have a random slot access using the main channel, and the traffic is sent in a virtual hopping channel (as in selective call mode), ensuring no risk of contention.



SYNC | ARQ SYNCH | MESSAGE | ARQ MESSAGE

Common channel: possible conflict

Channel dedicated to the transmit station: no conflict

2.5.8 Routing Principles

- Broadcast of tables at regular periods of time; and
- Flood-search algorithm to define the optimum routing.

Figure 2-15: PR4G SAP.

Chapter 3 – WLAN TECHNOLOGIES

In the early 1970's, the success of the Ethernet project at Xerox's Palo Alto Research Center as well as of other similar digital protocols brings the Local Area Networks (LANs) technology in both the public and corporate sectors. Standard LAN protocols, such as Ethernet, that operate at fairly high speeds bring digital networking to almost any computer. However, LANs are limited to the physical and hard-wired infrastructure of the buildings. The origins of wireless networking standardization can be traced to the late 1980s, motivated by FCC spread spectrum regulations in the 2.4 GHz range. In the 1990's, it has been shown that many network users and, more especially, mobile users in business, medical profession, factories and universities could find benefit from the Wireless LANs (WLAN) capabilities.

The installation of traditional wired LAN is not always practical or feasible (e.g. in old buildings, in factory floors, in trading floors, in trade shows, at conferences…). Therefore, in many cases, WLAN offers the connectivity and the convenience of wired LAN without the need for expensive wiring or re-wiring. Additionally, WLANs present the advantage to combine both the power of the wireless access and the mobile computing delivering high data rates. The major motivation and benefit of WLANs is the increased mobility and flexibility that it is offered to the user.

The primarily application of WLANs as a mean of connecting computers, has been stretched to larger applications. Presently, the market and target segments of the WLANs are seen as being corporate, public access and home/consumer product environments.

As mentioned previously, WLANs are also penetrating the hospital and university environments in which users are highly mobile.

The demand in wireless networks in home, known as Home Networking, is poised for take-off. The homes with multiple computers are looking for ways to communicate among computers and share resources such as files, printers and broadband Internet connections. Consumer oriented electronics devices such as games, phone are being added to home WLANs. The home networks will have to deliver multiple services and support a broad variety of media and computing devices as part of a single network.

In corporate/business environments, WLANs have a big potential. As for example, employees could bring laptop computers together to communicate and share professional information in an ad-hoc network configuration. The ad-hoc network configuration would allow any group of people to connect together without having to be connected via an access point to a wired network (infrastructure network).

More and more, the mobile professionals are looking for:

- Ubiquitous, available wireless public access to the Internet (IP) and to corporate intranets.
- Broadband speeds that could respond to their demand for data-intensive applications.
- Security and Privacy.
- Reasonable access charges.
- Consolidated Internet access billing per trip.

Indeed, the most valuable assets for those users would be to access remotely through the IP backbone, which would require typically high bandwidth (e.g. e-mail attachment downloading). Presently, this large data transmission exceeds the cellular networks capacity and WLANs is a perfect broadband complement for the operator's existing GSM and GPRS services in an indoor environment to answer to the strong demand for public wide-area Internet access. As such, WLANs could be considered as a public wireless broadband access technology. However, current WLANs products offer limited global user management features as well as modest authentication and roaming capabilities compared to traditional cellular networks. The security and privacy issues are seen as a bottleneck for the realization of public WLANs as well as the ability of public WLAN operators to provide coverage areas for potential users, which would also imply roaming between the operators.

Wireless interworking is also gaining high interest and is of major importance for seamless interoperability between the networks. Recently, Ericsson announced its GPRS-WLAN interworking solution to enable users to roam seamlessly between Wide-Area mobile Networks (Wireless WANs) and WLAN networks without interruption. With their H2U project, Telenor and Ericsson are also active in interworking between UMTS and WLAN. AT&T labs are looking more particularly to Internet Roaming and proposed an IP-based integrated architecture that provides seamless interworking across WLAN and cellular technologies and the IEEE 802.11 study groups (e.g. convergence/interworking on WLANs/WWANs) as well as ETSI HIPERLAN type 2 are addressing the wireless interworking aspects.

Appropriate WLAN architectures still have to be developed to allow all these capabilities. Actually, a high-data rate European standard (ETSI H/2) has been designed in that sense, to enable this interworking. Other working groups (more particularly the IEEE 802.11e working group) are working on proposals to support Quality of Services (QoS) and multimedia in their WLAN specifications. As already mentioned, this interworking is extremely important in the willingness to offer seamless interoperability between business, home and public environments. QoS and multimedia-capable networks are essential ingredients to offer residential customers video-on-demand, voice over IP (multimedia applications) and high-speed Internet access, which are of interest for broadband service providers.

The present and future WLAN terminal penetration creates a high business opportunity for mobile operators to extend their services to cover WLAN access. In the following, a brief presentation of the existing WLAN chipset and products is made and compared to the other wired and not-wired solutions on the market. Afterwards, the future potential services and the market forecast are covered more specifically to present the market potential and to underline the needs for WLAN service deployments by the service providers.

3.1 THE IEEE 802.11 FAMILY OF STANDARDS

The IEEE 802.11 family is an extension of Ethernet to wireless communication. It supports TCP/IP, but also handles other forms of networks like IPv6 for enhanced mobile IP features. There are two physical layer standards: 802.11b operating in the 2.4 GHz radio band and 802.11a operating in the 5 GHz radio band. Products complying with 802.11b go through market in 2001. Products complying with 802.11a started to appear in North America toward the end of 2001. In many other countries, including those in Europe, regulators of radio spectrum block the use of 11a products operating in the 5 GHz radio band. A third physical layer specification, 802.11g, is in the final stages of being defined.

Other 802.11 standards (802.11c, d, e, f, g, h, i) extend the physical layer options, improve security, add quality of service (QOS) features or provide better interoperability. These are discussed below. Vendors proprietary implementations exist, in some cases before the IEEE has finalized the relevant standards.

The set of the IEEE 802.11 protocols and evolution are given below in the context of the layered model.

Table 3-1: WLAN Layered Model

MAC	**802.11** MAC	802.11 e MAC Enhancements – QoS	
		802.11f Access Point Interoperability	
		802.11i Enhanced Security Mechanisms	
PHY	Infrared (IrDA)	802.11 IrDA (1/2 Mbps)	
	2.4 GHz (FHSS) Frequency Hopping Spread Spectrum	802.11 FHSS (1/2 Mbps)	
	2.4 GHz (DSSS) Direct Sequence Spread Spectrum	802.11 DSSS (1/2 Mbps)	
		802.11b Extension (5.5 / 11 Mbps)	802.11g >20 Mbps
	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing	802.11a 6/54 Mbps Extension	802.11h Spectrum Management
			5 GHz Globalization

Main technical 802.11 characteristics are as follows:

- Bandwidth: Originally 1,2 Mbps (BPSK and QPSK), then CCK 5.5 and 11 Mbps.
- Asynchronous, connectionless service.
- Supports both ad-hoc and infrastructure mode operation.
- Spread Spectrum without requiring licensing.
- Three Physical Layer Implementations: **Direct Sequence Spread Spectrum** (DSSS), **Frequency Hopping Spread Spectrum** (FHSS), 915 MHz, 2.4 GHz (Worldwide ISM), 5.2 GHz, and **Diffused Infrared** (850 – 900 nm) bands (see more below).
- Multiple priorities supports.
- Time-critical and data traffic support.
- Power management allows a node to doze off.

3.1.1 IEEE 802.11b

One of the most used WLAN technologies is defined in IEEE 802.11b. The standard was completed in 1999 and a wide range of products exists since 2001. For radio access this standard defines three Frequency Hopping CDMA coded channels in unlicensed 2,4 GHz frequency band. It allows the wireless transmission of approximately 11 Mbps of raw data at distances from tens up to hundred meters. The distance depends on impediments, materials, and line of sight while the transmission rate depends strongly on usage of common unlicensed radio channel. Most wireless LAN installations today comply with 802.11b, which is also the basis for Wi-Fi certification from the Wireless Ethernet Compatibility Alliance (WECA).

The problem with this technology is unsatisfactory security. Many severe weaknesses in Wired Equivalent Privacy (WEP) have been identified, which is supposed to secure WLAN communication but does not deliver what its name implies.

The initial version of the IEEE 802.11b achieves only 1 Mbps with BPSK and 2 Mbps with QPSK over both FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). The task group for 802.11b was responsible for enhancing the initial 802.11 DSSS PHY to include 5.5 Mbps and 11 Mbps data rates to finalized the standard (IEEE Std. 802.11b-1999) in late 1999. At present FHSS is not longer used. To provide the higher data rates, 802.11b uses CCK (Complementary Code Keying), a modulation technique that makes efficient use of the radio spectrum.

It utilizes Direct Sequence Spread Spectrum (DSSS).

- Higher-Speed Physical Layer Extension of 802.11 in the 2.4 GHz Band.
- Use High Rate Direct Sequence Spread Spectrum (HR/DSSS).
- HR/DSSS uses the same PLCP preamble and header as DSSS, so both PHYs can co-exist in the same AP.
- Multirate: 1, 2, plus 5.5 and 11 Mbps, rate switching mechanism.
- Use Complementary Code Keying (CCK) modulation with 8 chip for high rates.

The DSSS provides an immunity of the WLAN signal from the noisy ISM band of the 2.4 GHz. The major interferences for the WLAN are the microwave ovens and other industrial applications.

The main DSSS characteristics employed are:

- Spreading factor = Code bits/data bit, 10 – 100.
- Commercial (Min 10 by FCC), 10,000 for military.
- Signal bandwidth >10 × data bandwidth.
- Code sequence synchronization.
- Correlation between codes.
- Signal modulated with a spreading code (11-bit Barker Sequence).
- All 802.11b compliant products use the same spreading code.
- Higher data rates because of “fatter pipe” (about 11 MHz).
- Allows for some single frequency noise and higher wideband noise.
- Only allows for 3 networks in same area.
- Uses higher power to transmit and more expensive to build than FHSS.
- Differential Binary Phase Shift Keying (DBPSK) for 1 Mbps, Differential Quadrature Phase Shift Keying (DQPSK) for 2 Mbps.

The Multiple Access Scheme employed has the following features:

- Two access methods: Distributed and Point Coordination Function.
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- Not all stations can hear each other (hidden station problem).

- CA: Listen before you talk. If the medium is busy, the transmitter backs off for a random period. However CA cannot detect collision, hence each packet is acked. If not acked, MAC level retransmission occurs.
- Avoids collision by sending a short message: Ready To Send (RTS), which contains source/ destination addresses and duration of message. Destination then sends Clear To Send (CTS) and all stations receiving RTS and/or CTS set their timer.
- NAV (Network Allocation Vector) for the given duration.

Two Supported Topologies exist: Ad-hoc and Infrastructure.

3.1.2 IEEE 802.11a

IEEE 802.11a defines an updated version of 802.11b standard in order to achieve higher data rates and enhanced security. The standard has been completed in 1999 and products are available now. The 802.11a uses 8 – 12 available radio channels in the low – medium UNII frequency band at 5.2 GHz and achieves data throughput up to 54 Mbps. Products based on the IEEE’s 802.11a standard cannot interoperate with slower 802.11b units because they run on different bands. The 802.11a standard is using Orthogonal Frequency Division Multiplexing (OFDM). 802.11a supports data rates ranging from 6 to 54 Mbps.

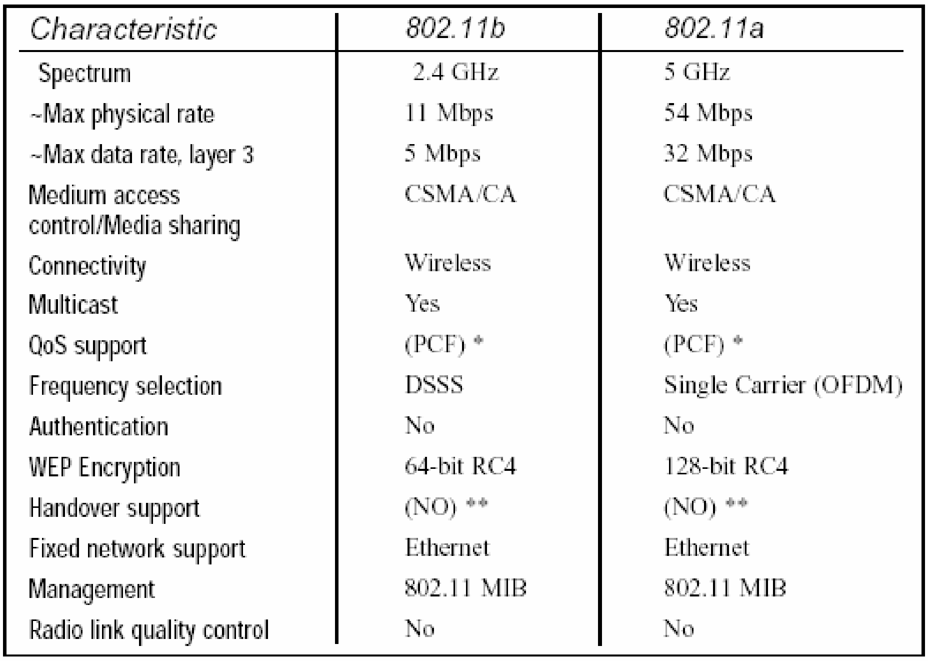
Because of operation in the 5 GHz bands, 802.11a offers much less potential for radio frequency (RF) interference than other PHYs (e.g. 802.11b and 802.11g) that utilize 2.4 GHz frequencies. With high data rates and relatively little interference, 802.11a does a great job of supporting multimedia applications and densely populated user environments. This makes 802.11a an excellent long-term solution for satisfying current and future civilian requirements.

It specifies 8 available radio channels (available radio spectrum in some countries would permit the use of 12 channels – the US 5 GHz Unlicensed Band supports 12 non-overlapping 802.11a networks).

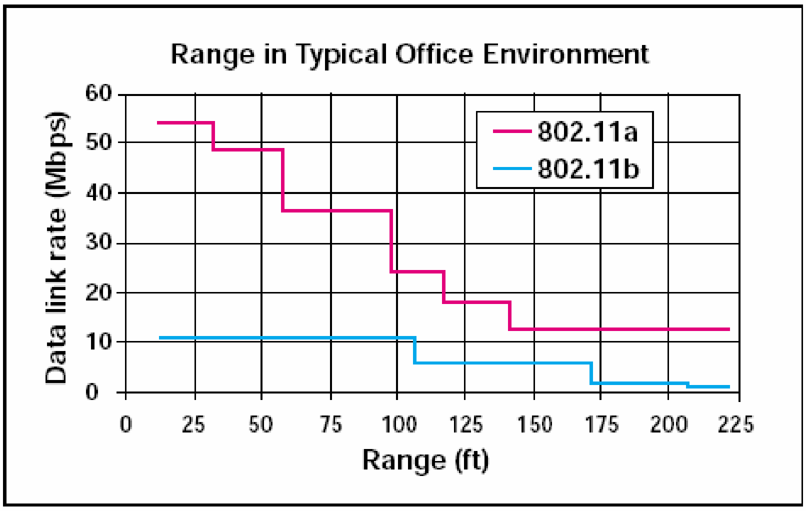
The benefits of 802.11a are:

- Significantly higher data rates, up to 54 Mbps.
- Operating at comparable range and faster speeds than 802.11b.
- Allows users to perform bandwidth intensive applications without sacrificing throughput.
- Increased scalability, better interference immunity.
- 802.11a supports many more channels (8 non-overlapping instead of 3 with 802.11b).
- OFDM modulation scheme.
- Within a channel, the 20 MHz spectrum is divided into 52 “narrowband carriers” each about 300 KHz, based on OFDM technology.
- The high data rate is accomplished by combining many lower-speed subcarriers to create one high-speed channel.

Table 3-2: IEEE 802.111/b Characteristics



Characteristic	802.11b	802.11a
Spectrum	2.4 GHz	5 GHz
~Max physical rate	11 Mbps	54 Mbps
~Max data rate, layer 3	5 Mbps	32 Mbps
Medium access control/Media sharing	CSMA/CA	CSMA/CA
Connectivity	Wireless	Wireless
Multicast	Yes	Yes
QoS support	(PCF) *	(PCF) *
Frequency selection	DSSS	Single Carrier (OFDM)
Authentication	No	No
WEP Encryption	64-bit RC4	128-bit RC4
Handover support	(NO) **	(NO) **
Fixed network support	Ethernet	Ethernet
Management	802.11 MIB	802.11 MIB
Radio link quality control	No	No



Source: Atheros Communications Inc.

Figure 3-1: WLAN Range.

3.1.3 Bridge Operation Procedures with 802.11c

IEEE 802.11c is a set of instructions named "Support of the Internal Sub-layer Service by Specific MAC Procedures to cover bridge operation with IEEE 802.11 MACs". It will not be published as a separate document.

802.11c provides required information to ensure proper bridge operations. This project is completed, and related procedures are part of the IEEE 802.11c standard. Product developers utilize this standard when developing access points. This standard is not of primary concern to wireless LAN installers.

3.1.4 Global Harmonization with 802.11d

IEEE 802.11d promotes worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.

When 802.11 first became available, only a handful of regulatory domains (e.g. U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory requirements within a group of additional countries. This is especially important for operation in the 5 GHz bands because the use of these frequencies differ widely from one country to another.

In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products nor do users accept the need to cope with several country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.

Work is ongoing, but see 802.11h for a timeline on 5 GHz WLANs in Europe.

3.1.5 Enhancements for QoS with IEEE 802.11e MAC

IEEE 802.11e is a supplementary to the MAC layer to provide QoS support for LAN applications. It will apply to 802.11 physical standards a, b and g. Its purpose is to provide classes of service with managed levels of QoS for data, voice and video applications.

Without strong quality of service (QoS), the existing version of the 802.11 standard is not optimized for the transmission of voice and video. There is a lack of effective mechanism to prioritize traffic within 802.11. As a result, the 802.11e task group is currently refining the 802.11 MAC (Medium Access Layer) to improve QoS for better support of audio and video (such as MPEG-2) applications. The 802.11e group should finalize the standard by the end of 2002, with products probably available by mid-2003.

Because 802.11e falls within the MAC Layer, it will be common to all 802.11 PHYs and be backward compatible with existing 802.11 wireless LANs. As a result, the lack of 802.11e being in place today does not impact a decision on which PHY to use. In addition, the aim is to offer upgrades of existing 802.11 access points to comply with 802.11e through relatively simple firmware add-ons.

3.1.6 An Inter Access Point Protocol with IEEE 802.11f

IEEE 802.11f is a “recommended practice” document that aims to achieve radio access point interoperability within a multivendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.

The existing 802.11 standard does not specify communications between access points in order to support users roaming from one access point to another. The 802.11 WG purposely did not define this element in order to provide flexibility in working with different distribution systems (i.e. wired backbones that interconnect access points). Hence access points from different vendors may not interoperate when supporting roaming. The inter access point protocol is the scope of 802.11f so as to provide the necessary information that access points need to exchange to support the 802.11 distribution system functions (e.g. roaming). The 802.11f group expects to complete the standard by the end of 2002, with products supporting the standard by mid-2003.

3.1.7 Higher Rate Extensions in the 2.4 GHz Band with IEEE 802.11g

802.11g is an extension to 802.11b. The 802.11g task group aims to develop a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. 802.11g will implement all mandatory elements of the IEEE 802.11b PHY standard. For example, an 802.11b user will be able to associate with an 802.11b access point and operate at data rates up to 11 Mbps. In early 2002, 802.11g decided to use OFDM instead of DSSS as the basis for providing the higher data rate extensions. A big issue with 802.11g, which also applies to 802.11b, is considerable RF interference from other 2.4 GHz devices, such as the newer cordless phones.

The transmitted signal uses approximately 30 MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

The FCC (Federal Communications Commission) still needs to approve the use of OFDM in the 2.4 GHz band. As a result, it will likely take a relatively long period of time before 802.11g products appear on the market.

Because of the earlier time to market and superior performance capacity, 802.11a rather than 802.11g will likely dominate the high performance WLAN market in the near-term and distant future.

Benefits:

- Includes all of 802.11b plus higher speed options based on new baseband;
- Enhanced Speeds 24, 36, 48, 54 Mbps;
- Enhanced Modulation –OFDM (same as 802.11a); and
- Spectrum 2.4 GHz.

3.1.8 Spectrum Managed 802.11a with 802.11h

IEEE 802.11h standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimise interference with other systems, particularly radar.

802.11h addresses the requirements of the European regulatory bodies. It provide dynamic channel selection (DCS) and transmit power control (TPC) for devices operating in the 5 GHz band (802.11a). In Europe, there’s a strong potential for 802.11a interfering with satellite communications, which have “primary use” designations. Most countries authorize WLANs for “secondary use” only. Through the use of DCS and TPC, 802.11h will avoid interference in a way similar to HiperLAN/2, the European-based competitor to 802.11a. 802.11h hopes to have their standard finalized sometime before the end of 2003.

To implement DCS and TPC, 802.11h is developing associated practices that affect both the MAC and PHY Layers. The inclusion of DCS and TPC will likely enable 802.11h to become the successor to 802.11a. Fortunately, there shouldn’t be any issues of non-interoperability between existing 802.11a and 802.11h users and access points. The good news is that 802.11h is enabling sales of 802.11a networks in Europe, which will eventually result in higher sales volumes and lower prices.

A fast-dwindling group will continue to support the alternative HyperLAN standard defined by ETSI. Although European countries such as The Netherlands and the United Kingdom are likely to allow the use of 5 GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003, possibly longer.

The standard is expected to be finalized by the second half of 2002. Products will be available in the first half of 2003 (firmware implementation), with high availability in the second half of 2003 (0.7 probability).

3.1.9 MAC Enhancements for Enhanced Security with 802.11i

IEEE 802.11i is a supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b and g. It provides an alternative to WEP with new encryption methods and authentication procedures.

As a conclusion over IEEE 802.11 standards it should be noticed that wireless communication is always more vulnerable and less reliable than its wired counterpart. Especially when using commonly available unlicensed frequencies the coverage of all possible communicating devices must be considered. Many technological obstacles must be overcome in order to achieve needed throughput with acceptable security. The familiar and widely used WLAN is good example of that. In practical networks many test have shown that actual throughput won’t be more than half of promised bit rate. Many security flaws have been found. To enhance the technology to meet the needs for better throughput and security many new additional standards have been introduced.

802.11i is actively defining enhancements to the MAC Layer to counter the issues related to wired equivalent privacy (WEP). The existing 802.11 standard specifies the use of relatively weak, static encryption keys without any form of key distribution management. This makes it possible for hackers to access and decipher WEP-encrypted data on your WLAN. 802.11i will incorporate 802.1x and stronger encryption techniques, such as AES (Advanced Encryption Standard).

It is not expected 802.11i to be available in the near future. The standard will likely not have IEEE ratification before mid-2003. 802.11i updates the MAC Layer, so you should be able to upgrade existing access points with firmware upgrades. The implementation of AES, however, may require new hardware.

For now, stronger forms of security that go well beyond WEP by implementing proprietary security mechanisms available from access points vendors. The problem is that you’ll probably need to deploy network cards and access points from the same vendor. As a minimum, utilize WEP.

The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2002. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility.

Finalization of the TKIP protocol standard is expected in the first half of 2002. Firmware will be available in the second half of 2002 (0.8 probability). The second half of 2003 expects new silicon with an AES cipher.

3.2 A BACKUP WIRELESS LAN FOR THE CZECH ARMY

3.2.1 Introduction

This chapter describes development steps on the way from the decision to the realization of new LAN communication facilities in the battlefield environment. These steps were made by Military Technical

Institute of Electronics in Prague (“VTÚE Praha”) during 2000 – 2001 years and were made in the frame of the giant and long-term project dedicated to the Czech Ground Forces Tactical Command and Control System (GF-TCCS).

One of the sub-task was find solution how to use the latest communication technologies on behalf of the modernization of the current Theater Operation Centers (TOC) on the Battalion level. The final goal was to design and realize one prototype of TOC using new LAN/WLAN technology.

These TOCs are designed on the base of shelters (topologically relatively isolated) on mobile platform (in vehicles). Each TOC consists of four (or more, max. 7) shelters (vehicles), which should be logically (one IP address space) connected together with versatile LAN by using fiber optics (FO), metallic cables and wireless technology (as a “warm” backup of FO). The fifth vehicle has special function and serves as an access node to support the communication to the upper operation level (to the Brigade via IP routers with ISDN/BRI interfaces).

Projected LAN is base on basics NATO standards (for example STANAG 4290 – NATO Multi-channel Tactical Digital Gateway – Cable Link (Optical) Standards) – to ensure interoperability and to fulfill high transfer rates for all possible types of data transfers (primary data, voice only in the case of using FO segments). These requirements led to the structure described below.

The structure of LAN consists of two types of LAN segments: internal LAN segments and external LAN segments. Internal segments of LAN are based on UTP or STP (twisted pairs) cables (10BaseT or 100BaseT) and are located inside the shelters. External LAN segments are FO (100(1000) Base FX, or 10Base FL) or WLAN and must be weather resistant. In the case of external LAN segments we decided to use FO (Fiber Optics) technology (base on STANAG 4290) with combination of WLAN (IEEE 802.11b).

Main requirements to the external LAN segments are following:

- FO LAN should be primary communication medium and should have the highest “communication” priority.
- Wireless technology should serve as “warm” backup of FO cables.
- WLAN “segments” should maintain rapid functionality of LAN after taking positions of shelters in terrain.
- FO and wireless technology must coexist and switching between them must be automatic.

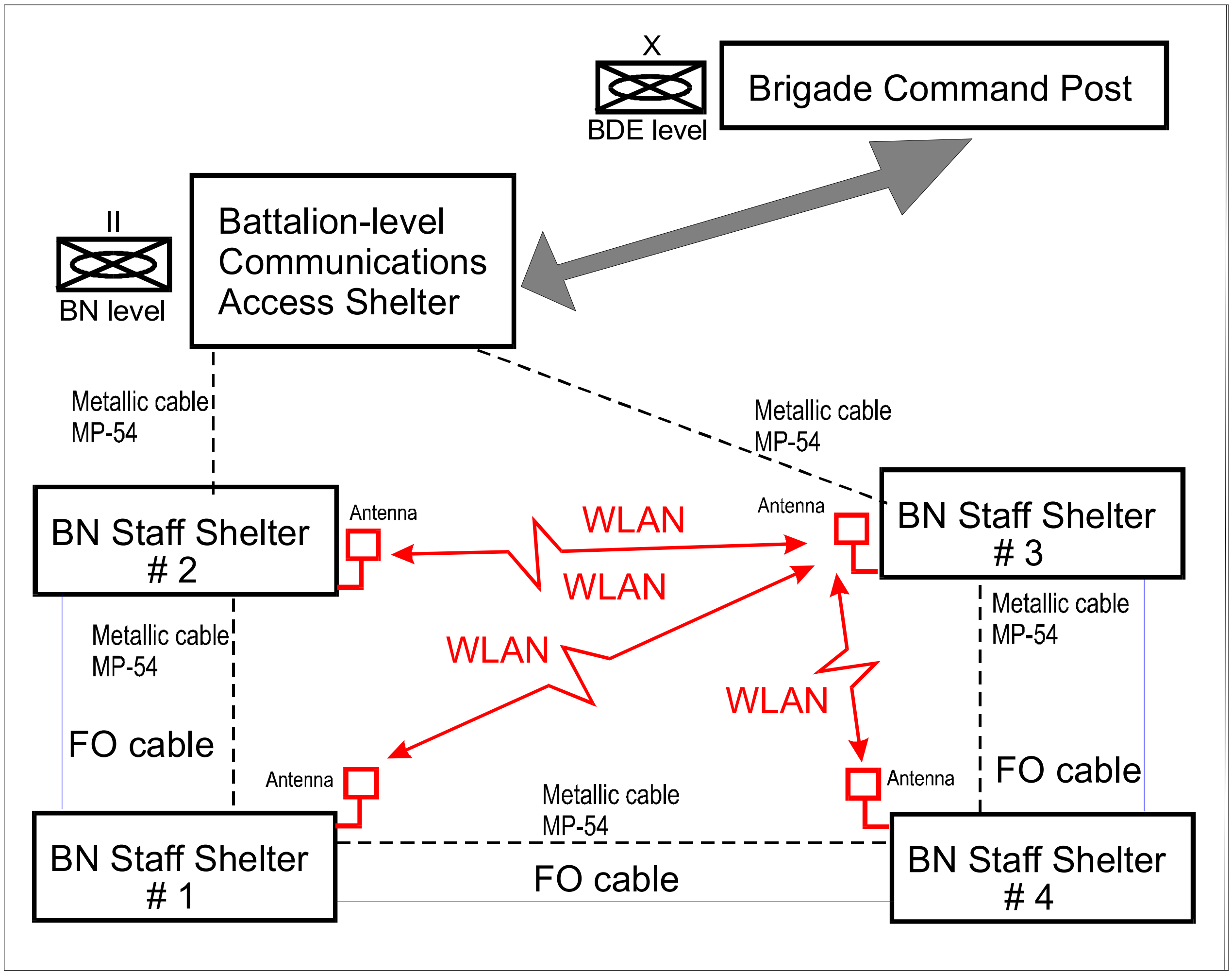


Figure 3-2: Battalion TOC LAN External Segment Layout (Simplified).

Remark: Metallic cables MP-54 between staff shelters (#1 – #2, #1 – #4, #3 – #4) serve to the analog telephones and as a transport medium for another legacy communication means.

In the case of communication between staff shelter #2 and communications access shelter (or between staff shelter #4 and communications access shelter) is the situation quite another. Here are metallic cables MP-54 used for two independent ISDN/BRI interfaces between Cisco routers (located in staff shelters #2, #3) and ISDN PABX (located in communication access shelter).

3.2.2 WLAN Step 1 – What is Available on the Market? Choosing COTS (Commercial Off The Shelf) Technology

The system architect and communication designer first considered to use the COTS technology “Bluetooth”, but the too short range (less then 10 m) was against the usage of it. (Staff shelters on Battalions TOCs could be more distant, the typical theoretical distance is approx. 500 m, but as will describe later, this factor wasn’t been fulfilled).

The second possibility was to use “pure” IEEE 802.11b standard WLAN technology in spite of the fact, that typical range is from tens up to hundred meters and depends on environment (trees, bushes, etc.) and materials in line of sign visibility.

Cisco Aironet WLAN appliances of series 340/350 (wireless bridge and wireless workgroup bridge) has been chosen for the experiments, but it was necessary to test the range (with directional and omni-directional antennas) in the real terrain before using of Aironet bridges in the field.

3.2.3 WLAN Step 2 – Distance and Reliability Measurement of Chosen Technology

The measurement should discover affect of bush and trees to the effective range of Aironet 340 with external antennas (omni-directional or directional).

Following three criteria of measurement were appointed:

- Criterion A: Level of signal measured by diagnostic utilities of Aironet system.
- Criterion B: Reliability of data transfers during transmission of 20 Mbytes long files.
- Criterion C: Error rate and average effective data rate.

Following equipment were used to the measurement:

- 2 pieces of WLAN bridges Cisco Aironet 340.
- 2 pieces of notebooks with Ethernet port 10 Mbit (10BaseT).
- 2 pieces of omni-directional antennas S24003BP (3 dB).
- 2 pieces of directional antennas HGY-15 (11,3 dB/30°).
- Antenna cables (6 m and 15 m).

There were chosen one common "typical" type of vegetation during spring season (without leaves) with following description:

- Wild leafy wood (hornbeam, beech).
- Quite dense (but person can go through).
- Dense branches in the height approx. 2 m above the earth.
- Diameter of trunks from 5 to 15 cm.

The testing place was prepared in a following manner:

- Both antennas (directional and omni-directional) were mounted on poles 2.5 m high to imitate the roof of vehicles.
- One place was used as **stationary measurement point** (with presence of experimentalists).
- The second place was used as **mobile point** with the notebook with hard disc (mapped as shared).
- Transmit rate was fixed at 11 Mbit/s.

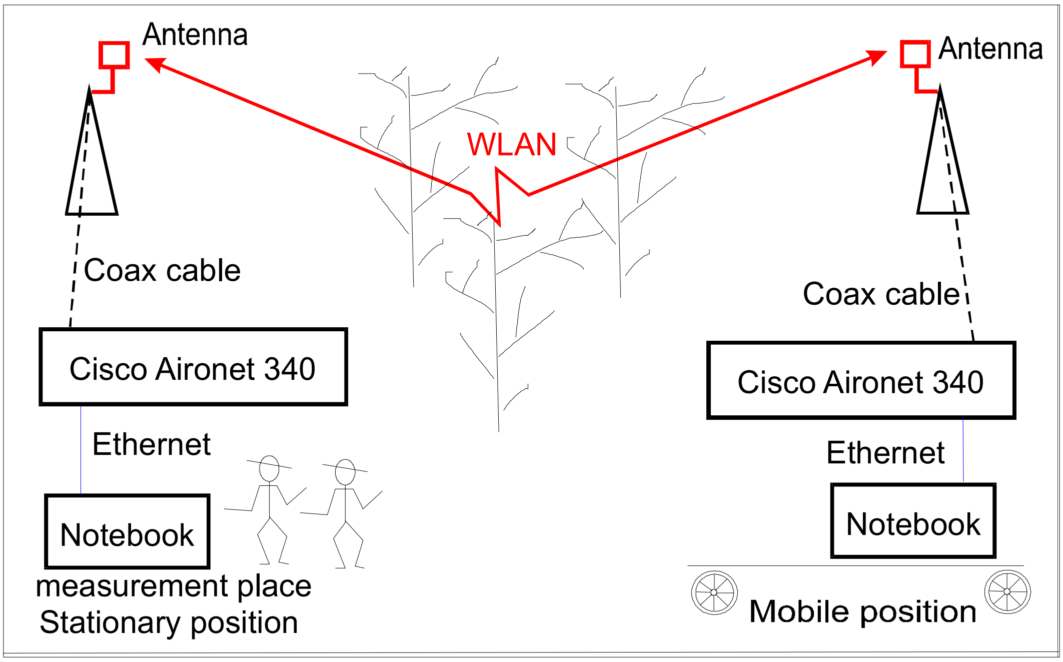


Figure 3-3: Diagram of Apparatus in the Terrain.

First measurement of range was done **in free space** (in the terrain without impediments of vegetation). Both points (stationary and mobile, **distance 160 m**) were equipped by **omni-directional antennas**. Results are here:

- Criterion A: with 50 mW output level of signal – without noticeable loss of signal.
- Criterion A: with 5 mW output level of signal (on both sides) – loss of signal to 50%.
- Criterion B: transfer of file (by 5 mW) was always successful.
- Criterion C: error factor = several dozens of bytes / 20 Mbytes, effective transfer rate 470 Kbytes/s.

Second measurement of range was done in the terrain **"through" the vegetation**. Both points (stationary and mobile) were equipped by **omni-directional antennas** too. Results are here:

- Criterion A: with 20 mW output level of signal by distance 30 m was noticeable loss of signal, with 50 mW by distance 40 m was loss of signal to 50%.
- Criterion B: Unstable file transfer with drop outs, transfer was very often timed out due to loss of synchronization of radio parts of Aironets.
- Criterion C: error factor was approximate 3% from 20 MB file, effective transfer rate around 100 kbytes/s.

Third measurement of range was done in the terrain **"through" the vegetation**. Both points (stationary and mobile) were equipped by **directional antennas** and by using **full output power 50 mW**. Results are here:

- Criterion A: loss of signal 50% in distance of 120 m.
- Criterion B: transfer of file was always successful.
- Criterion C: error factor = several hundreds of bytes / 20 Mbytes file, effective transfer rate around 450 kbytes/s.

Fourth measurement of range was done in the terrain “through” the **vegetation (sporadic bush)**. Both points (stationary and mobile) were equipped by **omni-directional antennas** and by using **full power 50 mW**. Results are here:

- Criterion A: loss of signal 50% in distance of 40 m.
- Criterion B: transfer of file was always successful.
- Criterion C: error factor = several hundreds of bytes / 20 Mbytes file, effective transfer rate around 450 kbytes/s.

The measurements (described above) led to following conclusions:

- Vegetation has drastic impact on range especially by using omni-directional antennas.
- Range of omni-directional antenna is influenced much more by trunks of trees then by thin branches of bush (difference is in accidental drop outs not in the level of signal).
- Range of directional antennas in density vegetation is more then 100 m.
- If vehicles (shelters) are grouped to the close quarters – is using of omni-directional antennas more practical (especially by the central vehicle).
- For standalone vehicles (shelters) would be good to use mechanical robust directional antennas.

In spite of the fact, that the range of WLAN (based on Cisco Aironet series 340/350) was in ideal case (free terrain without vegetation) about 160 m and in the worse case (vegetation) about 40 m, system architect and communication designer decided to use WLAN on technological platform IEEE 802.11b for prototype of TOC on battalion level. The advised tactical distance about 500 m between staff shelters wasn’t been fulfilled, but there wasn’t another technical solution (how to do the WLAN backup of FO) in that time.

3.2.4 WLAN Step 3 – Realization Details

All LAN and all segments (internal and external) of prototype of TOC were build on the base of following components (basic building blocks):

- **Ethernet switches Catalyst 3500XK**. Each staff shelter was equipped by this switch. This switches were a hearts of Ethernet LAN 100Base-T in each shelter and built so internal LAN segments. On this LAN segments where connected two servers (in shelter #1 and #3) and a lot of PCs (notebooks) Compaq Armada (or notebooks Getac A-760). External FO cables as well as the Aironet bridges 340/350 were connected to these switches. The “warm” backup logic of switching from FO to WLAN (and vice versa) was built in these switches.
- **TCP/IP routers Cisco 2620** with ISDN/BRI interface were install in staff shelters #2, #3 to establish communication from command post to higher level via communication access point.
- **WLAN Cisco Aironet components** (standard IEEE 802.11b), 3 pieces of Cisco Aironet 340/350 **wireless workgroup bridges with antennas**, 1 piece of Cisco Aironet 340/350 **multi-functional bridge (access point) with antenna.**
- **FO cables for distances up to 500 m** (100 Mbit/s, 100BaseFX, standard IEEE 802.3).
- **FO cables for distances up to 2 km** (10 Mbit/s, 10BaseFL).
- Another special equipment inside the staff shelters:
  - two PC dedicated as **graphics workstations** (in shelters #1 and #3);
  - **color laser printer** (format A3) in shelter #1;

- three **monochromatic laser printers** (A4 format) in shelters #2, #3, #4;
- **data projector** – (operable in external or internal space) of shelter #2; and
- **interactive Smart Board** (in shelter #2).

All of shelters were equipped by **standard telephones** (2 pieces), **cable cross-connects** and **external cable panels.**

3.2.5 Conclusion

All above described experiments and measurements tried to answer to the basic question: "Is WLAN (following "pure" standard IEEE 802.11b) usable in military field environment (in real terrain) as an backup of FO cables?". The indisputably true answer is **No** (without some reasonable changes).

One problem is the **carrier frequency** (around 2.4 GHz, band of "microwave ovens") that is not a true military frequency band. Much more convenient would be to use the WLAN in military VHF/UHF bands around 225 – 380/400 MHz.

Another problem is the **maximal usable range** of IEEE 802.11b that is typically around 100 m. Some experts advise to use **lower frequency** – typically around 300 MHz. In this band (with the same output power of transmitter) we can prolong the range approximately ten times.

From tactical point of view it is necessary to consider that the distance of staff shelters should be around 500 m. In the ideal case the field "military" WLAN should have the typical range around 1000 m or a little bit more in the terrain with vegetation effects.

To prolong the range of WLAN we can **slow down the bit rate** from 11 Mbit/s to 1 Mbit/s and this bit rate is still sufficient for some modest military applications (but it is too little as an full backup of FO bit rate capacity).

Another way to prolong the range of "military" WLAN is to use **more HF output power** of transmitters. To use not only 50 mW or 100 mW, but 1 W or more.

Protection of military information in the point of security is another topic that is necessary to consider in the WLAN in field environment. But it goes above the frame of this testbed description.

Almost all here mentioned technical adaptations of WLAN for military application were proposed and described in Paper A-23: "Wireless Tactical Local Area Network" by Prof. Torleiv Maseng (Norway).

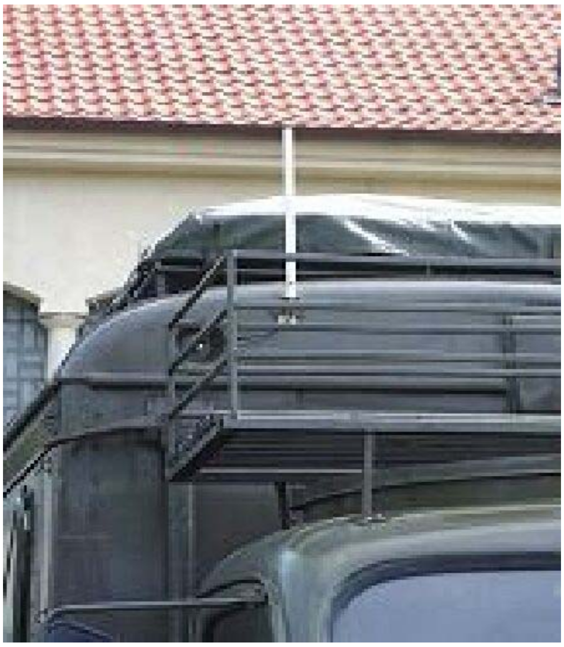


Figure 3-4: Detail View of Omni-Directional Antenna for WLAN on the Roof of Staff Shelters.

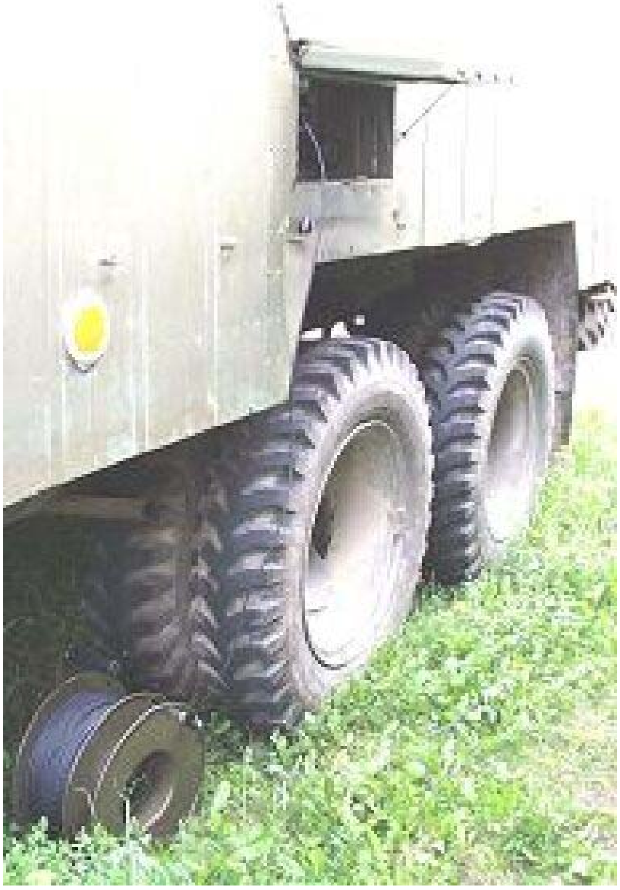


Figure 3-5: External Cable Panel with Connected FO Cable (on the reel).

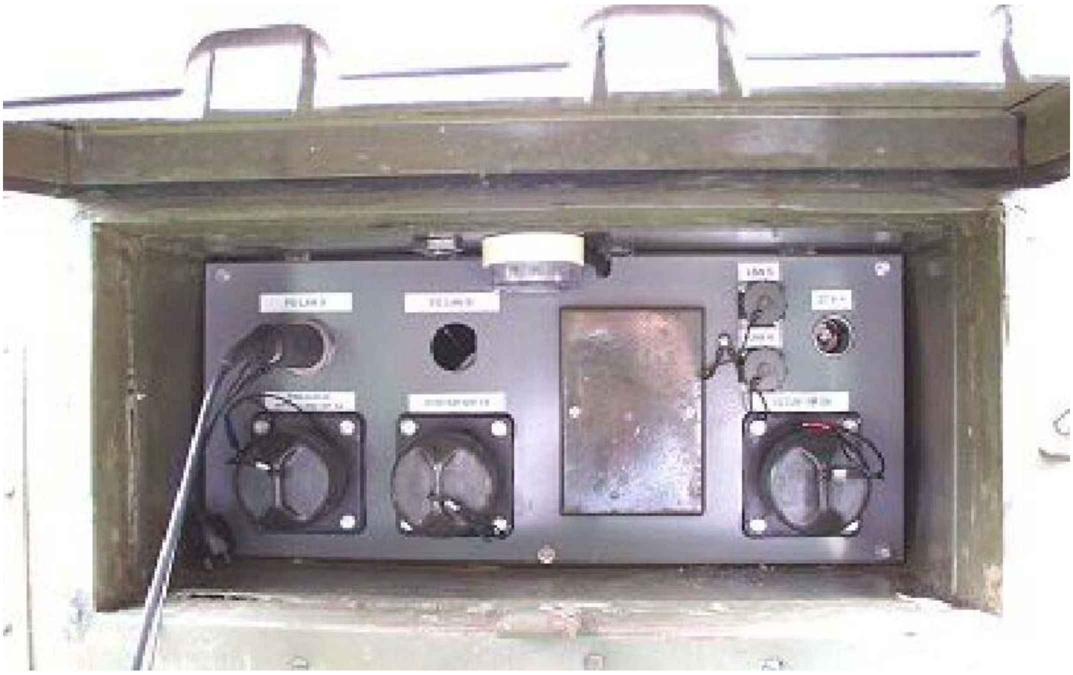


Figure 3-6: External Cable Panel – Detailed View.

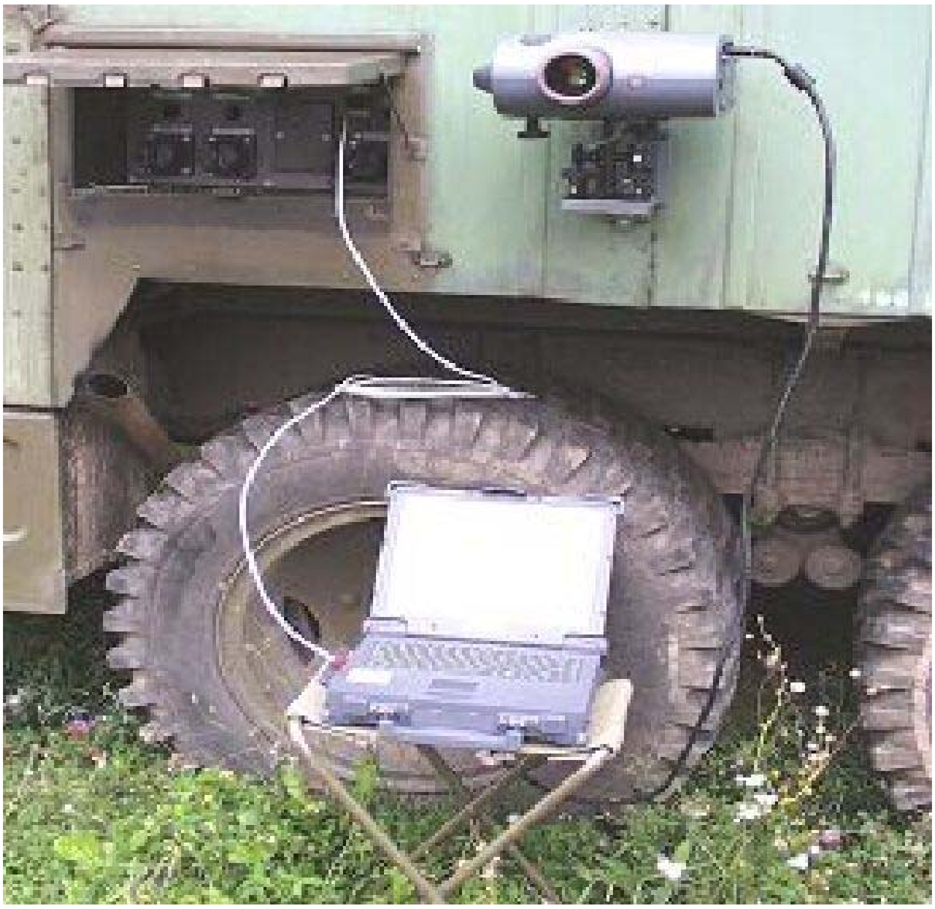


Figure 3-7: Connection of External Notebook GETAC with Data Projector to Shelter Cable Panel.

3.3 AN 802.11B RELATED EXPERIMENT AT FFI IN NORWAY

The purpose of the experiment was to increase the range of the WLAN cards.

In order to gain experience with the IEEE 802.11b cards, we made some small changes to a commercial card:

- We fixed the data rate to 1 Mbit/s. These cards are designed to work at 1, 2 5.5 and 11 Mbit/s adaptively depending on link propagation conditions. Ideally, we would like to reduce the rate, but this turned out to be tricky. We expect the coverage results to be improved and the rate to be increased if we had managed to reduce the rate.
- By disabling the diversity switch between two antennas on the card, we were able to convert the input and output frequency to around 300 MHz by an external oscillator and mixers.
- We increased the output power from 50 mW to 3 Watts.

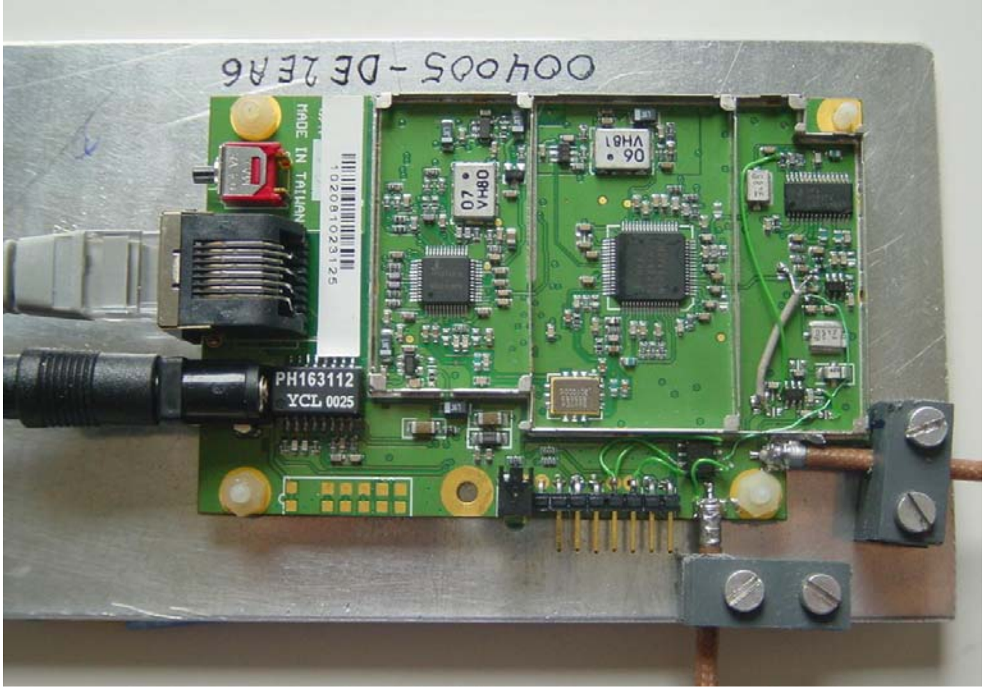


Figure 3-8: WLAN Experiment in FFI.

The WLAN card was equipped with two antenna connectors to provide diversity. These were used to transpose the carrier frequency from 2.45 GHz to 300 MHz. The adaptive bit rate was disabled and locked to 1 Mbit/s. The connectors on the left provide Ethernet and power. Extra equipment containing power, frequency converters and power amplifier is not visible.

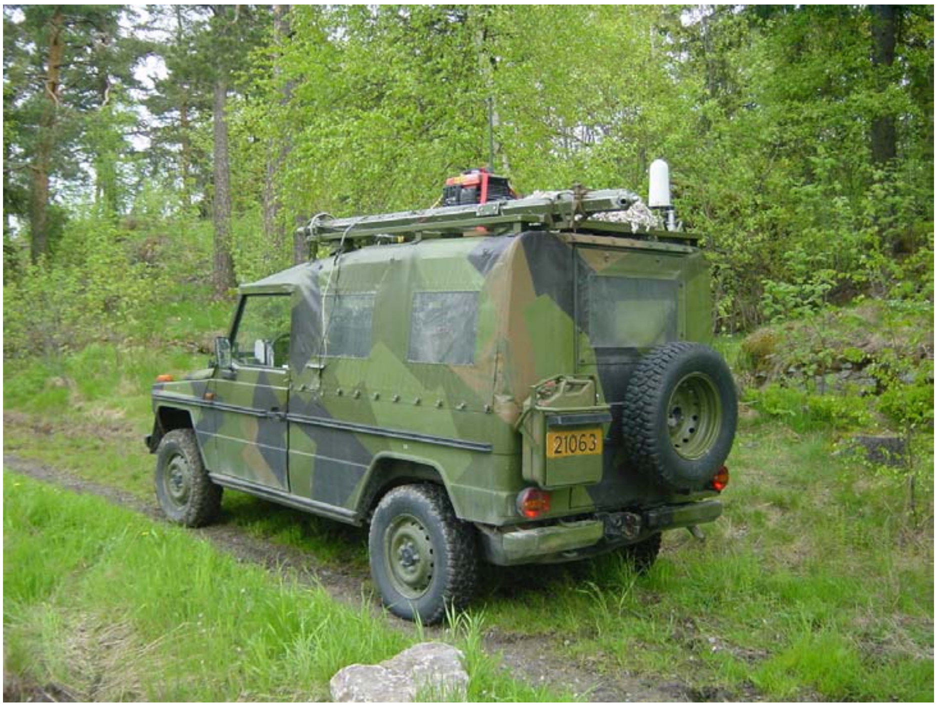


Figure 3-9*:* FFI Experiment.

On the figure two antennas can be seen. The white was used for experiments at 2.45 GHz and the green whip antenna (hardly visible in the center roof of the car) was used for 300 MHz.

3.3.1 Measurements

Measurements were made 17/4-2001 with two cars. One was acting as a transmitter and the other as a receiver. The link-analysis was done using a software computing package error rate (PER). The packages were send-using UDP (which is connectionless).

3.3.2 Specifications

Measured sensitivity at receiver: -99 dBm.

Output power: 3 W (35 dBm)

Data rate: 1 Mbit/s.

Package length: 1000 bytes.

Packages/second = 62

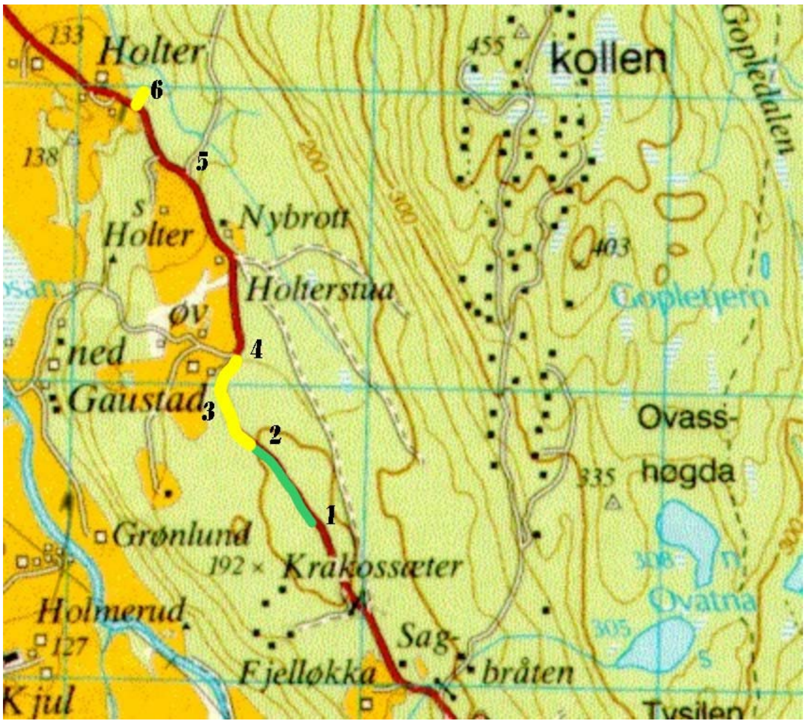


Figure 3-10: FFI Experiment – Route.

PT. 1: This position is just before the top of a small hill. The second car remained at Pt. 1 until Pt. 5.

PT. 2: The second car with the receiver drove from 1 to 2. Result: PER < 1% (green). Signal strength was better than -56 dBm. The distance between 1 and 2 is about 300 m with fairly dense wood.

PT. 3: From 2 and 3 is downhill. While signal strength is well above sensitivity limit since it was better than -73 dBm, the PER is varying between 0 and 100% (yellow), which indicates multipath problems. Maximum altitude difference was about 10 m.

PT. 4: Between 3 and 4 PER varies between 80 and 100%. Signal strength was –75 dBm and the distance between transmitter (at PT. 1) and receiver (at PT. 4) was now up to 600 m.

PT. 5: The measurements between PT. 5 and 6 in very dense wood. The second car was now stationary at PT. 5. The distance between the vehicles was now all the time around 200 m (indicated by yellow). Signal strength = -60 dBm. PER varies between 0 and 100%.

These measurements indicate that this system is very sensitive to multipath. With a rate reduction by a factor 8 this should be less of a problem.

Most of the features above are acceptable and even attractive in a tactical LAN, but not all. Assuming that an external crypto unit performing authentication and encryption can improve the security features, and the ESM and jamming threat can be accepted, it is still desirable to increase the range. Reducing the bit rate of IEEE 802.11b by a factor of 8, will improve the power budget and make the system able to handle longer multipath which otherwise would be a problem when the range is increased. Reducing the carrier frequency from 2.435 to 300 MHz will improve the range, in particular in forest. Besides, it is for many applications no problem to increase the transmit power. The result will be an increase in range by a factor of 10!

A continuation of this project is carried out by several nations. Some of the effort is reported at http://www.nc3a.nato.int/mwlan.html.

Chapter 4 – OVERVIEW OF 802.16 – MILITARY RELEVANCE

In the following pages, an overview of the 802.16 standards is provided. Broadband wireless access (BWA) and the related frequency bands used are first defined, and a brief history of BWA standards is presented. A more detailed analysis and overview of the multiple standards, activities and projects initiated within the 802.16 study group is then presented. These include the 802.16-2001 physical (PHY) and Medium Access Control (MAC) standard for the 10 – 66 GHz band, the 802.16a air interface for 2 – 11 GHz with the corresponding MAC enhancements, the recommended practice for coexistence of fixed broadband wireless access systems: 802.16.2-2001 (for 10 – 66 GHz) and the 802.16.2a (for 2 – 11 GHz). Work has also been initiated by the 802.16 group to cover Interoperability Testing (802.16c and 802.16d) and a set of Test Protocols are being developed for this purpose. Finally a mobility project has been initiated (802.16.e) to bring a level of portability or mobility into the standard.

At this time, very few (if any) commercial products follow the 802.16 standard, but many manufacturers have plans to migrate their systems to support the standard. One reason why so few commercial products support the standard is because the standard is very new, is changing, and for some frequency bands, is still under development.

Finally, it is seen that improved security measures at the MAC layer have been introduced for 802.16 (compared to previous standards such as 802.11b). These measures should satisfy the privacy requirements for commercial products but may not be sufficient for military applications.

An analysis is performed on the possibility of using the 802.16 commercial products for military communications. It is concluded that because this commercial standard is designed to meet each country's regulatory restrictions and minimize interference, it produces, by military standards, a non-robust (vulnerable) signal that could be a significant liability in many tactical situations. There is no doubt that the 802.16 standard physical layer is highly vulnerable to signal detection and interruption. Traditional EW techniques of detection, direction finding (DF), and jamming of such a non-robust signal should prove effective and within the capabilities of almost any conceivable adversary.

Because of the large range of the transmissions (a few kilometers), the 802.16 signal is particularly vulnerable since it is made available (for interception and detection) to anyone located within this large perimeter.

Notwithstanding the physical layer robustness issues, given that the 802.16 is a new, unproven standard, it is also recommended at this time to wait until its widespread deployment before considering it further for military applications. As we have seen with the 802.11 standard, the first and second generations of the standard implementations contained a number of weaknesses that are only now being corrected. Hence, given the limited availability of commercial systems that supports 802.16, the real weaknesses of 802.16 are expected to surface only later, when these systems become widely deployed, and when they are subjected to greater exposure and become the target of hackers.

4.1 BROADBAND WIRELESS ACCESS

Broadband wireless access (BWA) is directed at providing broadband data access to businesses and homes using an inexpensive wireless infrastructure. The goal is to provide an economical and competitive solution to wired and satellite broadband. The wireless infrastructure consists of fixed (stationary) customer premise units, served by fixed terrestrial base stations. Services typically include broadband Internet access, digital video and telephony. Supported protocol could include TCP/IP as well as ATM.

4.1.1 Frequency Bands for BWA

Various frequency bands have been allocated across the world to support broadband wireless access. For example, some of the allocations include:

- Millimeter wave bands:
    - 18 – 24 GHz, 26 GHz (ETSI), 27.5 – 29.5 GHz, 38 GHz (ETSI), etc.;
    - LMDS (28 and 31 GHz) in the U.S. and some other countries;
    - Largest spectrum in private hands; and
    - 25 times as large as PCS spectrum cap.
- Microwave (centimeter wave) bands:
    - 3.5 GHz in most countries, 10 GHz in some others; and
    - 2.5 GHz in the U.S. (MMDS) and some other countries.
- License-Exempt bands, e.g. in many countries:
    - 5.725 – 5.825 GHz, 5.15 – 5.35 GHz;
    - 2.4 GHz Wireless LANs; and
    - 57 – 64 GHz.

4.1.2 Broadband Wireless Access Standards History

A few projects were initiated to try to standardize the Physical (PHY) and MAC layers used for broadband wireless access. In particular, two of the major initiatives are:

- The Broadband Radio Access Networks (BRAN) initiative of the European Telecommunications Standards Institute (ETSI). It includes the HIPERACCESS and HIPERMAN standards (see below).
- The 802.16 initiative, started in the USA by Roger Marks, from the National Institute of Standards and Technology, U.S. Department of Commerce. This initiative started with a project development in the summer of 1988 and was followed by the creation of an IEEE study group that led to the formation of an IEEE 802.16 standard group[1]. Current and former membership of the 802.16 standard groups includes over 144 companies from 12 countries[2].

A very short description of HIPERACCESS and HIPERMAN is given below. Since the goal of this report is to study 802.16, the rest of this report will be dedicated to the IEEE standard.

4.1.3 Broadband Wireless Access in ETSI BRAN

- BWA effort share many features of HiperLAN2 (the 5 GHz WLAN solution).
- HIPERACCESS:
    - For frequencies above 11 GHz;
    - Line-of-sight connections, up to 5 miles (8 km) range;

[1] The main 802.16 web site is at web addresses: http://WirelessMAN.org or http://ieee802.org/16/.

[2] Countries of 802.16 Members (current and former, as of July 2002): Canada (48), Finland (4), France (2), Germany (2), Greece (2), Israel (22), Italy (1), Japan (2), Korea (4), Spain (1), UK (11), USA (161).

  - 25 to 60 Mbps data rates, using Single Carrier;
  - HIPERACCESS began before 802.16; and
  - HIPERACCESS is completing its work.

The current versions of HIPERACCESS Physical Layer specification (TS 101 999), the HIPERACCESS System Overview (TR 102 003) and the HIPERACCESS Data Link Layer specification (TS 102 000) can be found on the ETSI/BRAN web site[3].

- HIPERMAN:
  - For frequencies below 11 GHz;
  - Does not need line of sight, up to 15 miles (24 km) range;
  - 10 to 25 Mbps data rates; and
  - Selected 802.16 MAC/802.16a OFDM PHY as baseline.
- Harmonization efforts under way to have some degree of compatibility with 802.16.

The current versions of the "Functional Requirements for Fixed Wireless Access systems below 11 GHz: HIPERMAN" (TR 101 856), and the draft HIPERMAN Physical layer, Data Link Control (DLC) layer and System Reference documents can be found on the ETSI/BRAN web site[4].

4.2 THE 802.16 STANDARDS, PROJECTS AND ACTIVITIES

4.2.1 Scope of the IEEE 802.16

The IEEE 802.16 Working Group on Broadband Wireless Access Standards develops standards and recommended practices to support the development and deployment of broadband Wireless Metropolitan Area Networks (WMAN).

The 802.16 standard specifies the physical layer (PHY) and medium access control layer (MAC) of the air interface of interoperable point-to-multipoint broadband wireless access systems. The specification enables access to data, video, and voice services with a specified quality of service. The medium access control layer is structured to support multiple PHY specifications, each suited to a particular operational environment, both in licensed bands designated for public network access and in license-exempt bands. It applies to systems operating between 2 and 66 GHz, where such services are permitted.

The 802.16-2001 standard includes a particular physical layer specification applicable to systems operating between 10 and 66 GHz. This 10 – 66 GHz air interface, based on single-carrier modulation, is known as the WirelessMAN-SC air interface. An amendment to this standard, to support 2 – 11 GHz using an enhanced version of the same basic medium access control layer along with new physical layer specifications, is in development in Project 802.16a.

4.2.2 Overview of the 802.16 Standards, Projects and Activities

The IEEE Standard 802.16-2001 supports a point-to-multipoint topology in which each base station, normally connected to a public network, communicates with potentially hundreds of stationary subscriber stations, each of which is typically mounted on a rooftop. Through the WirelessMAN MAC, each base

[3] http://www.etsi.org/t_news/0202_bran.htm

[4] http://portal.etsi.org/bran/Summary.asp

station allocates uplink and downlink bandwidth to satisfy, almost instantaneously, the prioritized bandwidth requirements of the subscribers. The air interface is designed to carry any data or multimedia traffic with full Quality of Service (QoS) support. The MAC supports burst frequency-division duplex (FDD) and time-division duplex (TDD) in a consistent framework. It also supports real-time adaptive modulation and coding so that, in each burst, communication in the link to each subscriber station is optimized at that instant.

The IEEE Standard 802.16-2001 defines the WirelessMAN-SC air interface, a single-carrier (SC) modulation scheme for 10 – 66 GHz operation. At these frequencies, propagation is strictly line-of-sight, but tremendous spectral allocations such as 1.3 GHz of spectrum in the U.S. Local Multipoint Distribution Service (LMDS) allocation, are available. The standard takes full advantage of the allocations, specifying bit rates of up to 120 Mbps on each reusable 25 MHz channel. The primary markets will include commercial, industrial, and multi-tenant residential buildings. In further support of this industry, the 802.16 Working Group has completed IEEE Standard 802.16.2-2001, a Recommended Practice on Coexistence, and is currently developing, in Project 802.16c, system profiles for use in compliance and interoperability testing.

While the WirelessMAN MAC in IEEE Standard 802.16-2001 provides the foundation for a wireless MAN industry, the physical layer (PHY) is not suitable for lower-frequency applications, where the available spectrum allocations are narrower and near non-line-of-sight operation is possible. For this reason, most of the recent efforts in the 802.16 Working Group have gone toward the development of IEEE Project 802.16a, an amendment to address 2 – 11 GHz operation. Successive versions of the 802.16a draft have been in ballot since November 2001, and the details are nearing completion. The amendment includes both licensed and 5 – 6 GHz license-exempt bands. In the licensed bands, the current draft provides for compliance using any of three physical layer modes: single-carrier (SC) modulation, orthogonal frequency division multiplex (OFDM), or orthogonal frequency division multiple access (OFDMA), with advanced antenna options supported. For the license-exempt spectrum, the current 802.16a draft specifies the OFDM mode.

In license-exempt operation, wireless MANs are susceptible to interference with other wireless MANs as well as with other devices such as wireless LANs. As one solution to this problem, the 802.16a draft specifies a dynamic frequency selection (DFS) method for license-exempt bands similar to the one being standardized in IEEE Project 802.11h. The draft also supports the use of a mesh architecture in which some subscriber stations communicate with other data-forwarding subscriber stations rather than directly with the base station. This allows extending the cells and reaching customers not directly reachable from the base station. The defined scheduling algorithms provide for collision-free transmissions in mesh deployment. The protocols also eliminate the hidden-terminal problem typical of wireless LANs.

The work of the 802.16a group should be completed within the next few months. The next great hurdle for the 802.16 group is to bring a level of portability or mobility into the standard. To support this initiative the Working Group recently initiated the Study Group on Mobile Broadband Wireless Access (Project 802.16e), whose scope includes: “mobile broadband wireless access networks supporting mobility at vehicular speeds.”

One important new player is the Worldwide Interoperability for Microwave Access (WiMAX) Forum, whose mission includes promoting IEEE Standard 802.16 to achieve global acceptance as well as developing and implementing test procedures to ensure interoperability.

Related to interoperability, the 802.16 working group has initiated a series of projects to form the basis of compliance and interoperability testing. This work will include the production of a Protocol Implementation Conformance Statement (PICS) as well as a Test Suite Structure and Test Purposes document.

The activities of 802.16 and its various standards and projects are summarized in Table 4-1.

Table 4-1: Summary of 802.16 Standards, Projects (P) and Activities

IEEE 802.16 Standards, Projects(P) and Activities		
AIR INTERFACE STANDARD **(PHYs with common MAC)**	**802.16-2001** (10 – 66 GHz)	• MAC • PHY for 10 – 66 GHz • Approved by IEEE in Dec. 2001
	P802.16a amendments (2 – 11 GHz)	• MAC Enhancements • PHY for 2 – 11 GHz • Licensed and license-exempt bands • Draft 6 released in Oct. 2002 • Approval expected early 2003
COEXISTENCE **(Recommended Practice)**	**802.16.2-2001** (10 – 66 GHz)	• 10 – 66 GHz • Approved by IEEE in July 2001
	P802.16.2a amendments (2 – 11 GHz)	• Includes 2 – 11 GHz licensed • Draft 1 done in September 2002 • Completion expected mid-2003
Follow-up Projects		
Interoperability Testing	**P802.16c** (10 – 66 GHz)	• Used as basis of compliance and interoperability testing • Draft 4 released in Oct. 02 • Approval expected early 2003
	P802.16d (2 – 11 GHz)	• New project, to form the basis of 2 – 11 GHz interoperability testing.
Test Protocols **(10 – 66 GHz)**	**P1802.16.1**	• Protocol Implementation Conformance Statement (PICS) • Started; final expected early 2003
	P1802.16.2	• Test Suite Structure and Test Purposes (started Oct. 02)
Mobility **(initially for < 6 GHz)**	**MBWA** – Mobile Broadband Wireless Access **(P802.16e)**	• Study Group formed in Mar. 02 • To investigate mobility enhancements for 802.16a
Other Activities related to 802.16		
Forum for the coordination of interoperability testing	**WiMAX** Worldwide Interoperability for Microwave Access	• To certify the interoperability of BWA products and technologies under a global standard • Support 802.16 • Developing and submitting baseline test specs

4.3 SOME OF THE TECHNICAL CONSIDERATIONS OF 802.16-2001 (10 – 66 GHZ)

The IEEE 802.16-2001 standard[5] was approved by IEEE in December 2001. It specifies the air interface, including the MAC and PHY layers, of fixed point-to-multipoint broadband wireless access systems providing multiple services. The standard includes a particular physical layer specification broadly applicable to systems operating between 10 and 66 GHz.

4.3.1 Properties of IEEE Standard 802.16-2001

- Broad bandwidth:
  - Up to 134 Mbps in 28 MHz channel (in 10 – 66 GHz air interface).
- Supports multiple services simultaneously with full QoS:
  - Efficiently transport IPv4, IPv6, ATM, Ethernet, etc.
- Bandwidth on demand (frame by frame).
- MAC designed for efficient used of spectrum.
- Comprehensive, modern, and extensible security.
- TDD and FDD.
- Link adaptation: Adaptive modulation and coding:
  - Subscriber by subscriber, burst by burst, uplink and downlink.
- Point-to-multipoint topology.

4.3.2 More Technical Details

More technical details on the PHY and MAC layers of the 802.16-2001 standard are provided in Annex A and in Table 4-2 in the following section.

4.4 AMENDMENT PROJECT IEEE 802.16A – AIR INTERFACE FOR 2 – 11 GHZ

This standard will extend the IEEE 802.16 WirelessMAN standard for applicability to 2 – 11 GHz bands, both licensed and license-exempt, and provide a foundation for the expansion of wireless metropolitan area networks in residential neighborhoods. It will include Medium Access Control Modifications and additional Physical Layer Specifications for 2 – 11 GHz. This standard is still under development, with Draft 6 released in October 2002. Approval by IEEE is expected by the end of 2002 or early 2003.

- **Licensed Bands**

The 2 – 11 GHz bands provide a physical environment where, due to the longer wavelength, true LOS may not be totally necessary and multipath may be significant. The channel bandwidths used in this physical environment typically vary from 1.5 to 28 MHz. Channel bandwidths allowed shall be limited to the regulatory provisioned bandwidth divided by any power of 2 no less than 1.25 MHz.

[5] http://standards.ieee.org/getieee802/download/802.16-2001.pdf

- **License-Exempt Bands (primarily 5 – 6 GHz)**

The physical environment for the 2 – 11 GHz license-exempt bands is similar to that of 2 – 11 GHz licensed bands. However, the license-exempt nature introduces additional interference and co-existence issues, whereas regulatory constraints limit the allowed radiated power. In addition to the features of licensed band, the PHY and MAC introduce mechanisms such as:

- DFS (dynamic frequency selection) to detect and avoid interference; and
- Support for Mesh topologies.

4.4.1 P802.16a PHY Alternatives

The PHY layer varies according to different applications, band plans, and regulatory environments. The three 2–11 GHz air interface specifications suggested in the draft 802.16a standard are:

- WirelessMAN-SC: This uses a single-carrier (SC) modulation format.
    - TDMA (TDD/FDD)
    - BPSK, QPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM
    - Most vendors will use Frequency-Domain Equalization
- WirelessMAN-OFDM: This uses orthogonal frequency-division multiplexing with a 256-point transform. Access is by TDMA. This air interface is mandatory for license-exempt bands.
    - 256-point FFT with TDMA (TDD/FDD)
- WirelessMAN-OFDMA: This uses orthogonal frequency-division multiple access with a 2048-point transform. In this system, multiple access is provided by addressing a sub-set of the multiple carriers to individual receivers.
    - 2048-point FFT with OFDMA (TDD/FDD)

4.4.2 Key P802.16a MAC Features

- OFDM/OFDMA Support.
- ARQ.
- Dynamic Frequency Selection (DFS) for license-exempt.
- Optional Advanced Antenna System (AAS) support.
- Mesh Mode:
    - Optional topology for license-exempt operation only;
    - Subscriber-to-Subscriber (relay) communications; and
    - TDD only.

4.5 COMPARISON OF KEY FEATURES OF 802.16-2001 AND P802.16A

The features of the 802.16-2001 and Project 802.16a standards are summarized and compared in Table 4-2.

Table 4-2: Comparison of Key Features of 802.16-2001 and 802.16a

	802.16-2001	P802.16a – Licensed and Licensed Except (LE) Bands		
		SC	*OFDM*	*OFDMA*
Frequency Band	10 – 66 GHz	2 – 11 GHz	2 – 11 GHz	2 – 11 GHz
Data Rate	2 – 155 Mbps			
LOS consideration	LOS	Near-LOS	Near-LOS	Near-LOS
Typical channel bandwidth	20 – 28 MHz	1.5 – 28 MHz	1.5 – 28 MHz	1.5 – 28 MHz
Center frequency	Multiple of 250 kHz	No restriction as long as Quadrature modulation used	$5000+5n_{ch}$ (MHz) $n_{ch}=0,1,\ldots 199$ for LE bands	$5000+5n_{ch}$ (MHz) $n_{ch}=0,1,\ldots 199$ for LE bands
Uplink scheme	DAMA-TDMA	TDMA	TDMA	CDMA
Downlink scheme	TDM	TDM	TDM	TDM
Duplexing techniques	TDD, FDD, H-FDD	TDD FDD H-FDD	FDD, H-FDD, TDD (in LE bands, only TDD)	FDD, H-FDD, TDD (in LE bands, only TDD)
Uplink modulation type	QPSK, 16 QAM, 64 QAM	Block adaptive modulation	OFDM Data: QPSK, 16 QAM, 64 QAM	OFDM Data: QPSK, 16 QAM, 64 QAM
Uplink FEC code type	RS, RS+ convolutional, coding, RS+ Parity Check, Turbo code	RS, Pragmatic TCM, BTC, CTC (convolutional turbo code)	Concatenated RS+ convolutional coding, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC
Downlink modulation type	QPSK, 16 QAM, 64 QAM	Block adaptive modulation	OFDM QPSK, 16 QAM, 64 QAM	OFDM Data: QPSK, 16 QAM, 64 QAM
Downlink FEC code type	RS, RS+ convolutional, RS+ Parity Check, Turbo coding	RS, Pragmatic TCM, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC
MAC support of PHY	Unframed FDD, Framed FDD, TDD	TDD, FDD	TDD, FDD (in mesh mode = only TDD)	TDD, FDD (in mesh mode = only TDD)
MAC	Basic	Basic, (ARQ), (STC), (AAS)	*Licensed*: Basic, (ARQ), (STC), (AAS)	*Licensed:* Basic, (ARQ), (STC), (AAS)
			License-exempt: Basic, DFS, (ARQ), (STC), (MSH), (AAS)	*License-exempt:* Basic, DFS, (ARQ), (STC), (MSH), (AAS)

4.6 RECOMMENDED PRACTICE FOR COEXISTENCE OF FIXED BROADBAND WIRELESS ACCESS SYSTEMS – IEEE 802.16.2 AND P802.16.2A

The 802.16.2-2001 recommended practice[6] for the bands 10 – 66 GHz was approved by IEEE in July 2001. Amendments are under way in Project 802.16.2a to provide a recommended practice for coexistence in the bands 2 to 11 GHz.

4.6.1 802.16.2-2001

This Recommended Practice provides guidelines for minimizing interference in fixed broadband wireless access systems. Pertinent coexistence issues are addressed, and recommended engineering practices provide guidance for system design, deployment, coordination and frequency system usage. This document covers frequencies of 10 – 66 GHz in general, with particular focus on 23.5 – 43.5 GHz bands. If followed by manufacturers and operators, it should allow for a wide range of equipment to coexist in a shared environment with acceptable mutual interference.

4.6.2 P802.16.2a

The goal of this project is to amend the "Recommended Practice for Coexistence of Fixed Broadband Wireless Access Systems" above to include the frequency bands 2 – 11 GHz. It takes into consideration the coexistence issues with point-to-point systems utilized in these bands. Draft 6 of this recommended practice was completed in October 2002 and approval by IEEE is expected by the end of 2002 or early 2003.

4.7 INTEROPERABILITY TESTING AND TEST PROTOCOLS FOR 802.16

4.7.1 P802.16c (System Profiles for 10 – 66 GHz)

This project, which was officially initiated in May 2002, aims at fostering the development of interoperability tests for systems built to the 10 – 66 GHz WirelessMAN-SC air interfaces. Draft 4 was released in October 2002 and approval by IEEE is expected in early 2003.

- Used as basis of compliance and interoperability testing:
  - MAC Profiles: ATM and IP Packet; and
  - PHY Profiles: 25 and 28 MHz; TDD and FDD.

4.7.2 P802.16d System Profiles for 2 – 11 GHz

In September 2002, the 802.16 Working Group approved submission of proposed Project Authorization Request (PAR) P802.16d on 2 – 11 GHz System Profiles. This work is expected to form the basis of 2 – 11 GHz interoperability test specifications.

4.7.3 P1802.16.1 Test Protocols for 10 – 66 GHz

Project P1802.16.1 is to define a Protocol Implementation Conformance Statement (PICS). Proforma document for the WirelessMAN-SC air interface. A full proposed PICS draft was received as a contribution in the fall 2002, and a Call for Comments on it was issued. The document is called "Draft Standard for Conformance to IEEE Standard 802.16 – Part 1: Protocol Implementation Conformance

[6] http://standards.ieee.org/getieee802/download/802.16.2-2001.pdf

Statement (PICS) Proforma for 10 – 66 GHz WirelessMANTM-SC Air Interface". Completion is expected in 2003.

4.7.4 P1802.16.2 Test Suite Structure and Test Purposes

The Working Group approved submission of a PAR to initiate the P1802.16.2 "Test Suite Structure and Test Purposes" for the 10 – 66 GHz. This would be the second of three anticipated conformance and interoperability test documents for this band.

4.8 MOBILE BROADBAND WIRELESS ACCESS FOR 802.16A

In March 2002, the 802.16 working group formed the Mobile Broadband Wireless Access Study Group to investigate mobility enhancements to 802.16. This group will address enhancements to the IEEE 802.16a PHY/MAC to support nomadic and mobile operation, roaming, and cell-to-cell and sector-to-sector handoff capability as well as other protocol and MIB support.

In September 2002, the 802.16 Working Group endorsed a project prepared by the Mobile Wireless MAN Study Group. The proposed project P802.16e will amend IEEE Standard 802.16 by specifying "Physical Layer and Medium Access Control Modifications for Mobile Operation in Licensed Bands below 6 GHz".

4.9 WIMAX FORUM

As a non-profit organization, the objective of WiMAX is to promote wide-scale deployments of point-to-multipoint networks operating between 2.5 and 66 GHz by leveraging new global consensus standards (802.16) and certifying the interoperability of various products and technologies from multiple manufacturers.

- WiMAX[7] = Worldwide Interoperability for Microwave Access.
- Mission: To promote deployment of BWA by using a global standard and certifying interoperability of products and technologies.
- Principles:
  - Support IEEE 802.16:
    - Initially above 11 GHz, but now also includes 2 – 11 GHz;
  - Propose access profiles for the IEEE 802.16 standard;
  - Guarantee known interoperability level;
  - Promote IEEE 802.16 standard to achieve global acceptance; and
  - Open for everyone to participate.
- Currently Developing and submitting baseline test specifications.
- WiMAX comprises of industry leaders who are committed to the open interoperability of all products used for broadband wireless access.
- Will certify interoperability levels both in network and the cell.

[7] http://www.wimaxforum.org/about/index.asp

The Test specifications developed will be used to:

- Ensure that equipment and systems claiming compliance to the standard or a profile have been sufficiently tested to demonstrate that compliance.
- Guarantee that equipment from multiple vendors has been tested the same way, to the same interpretation of the standard, increasing the interoperability of the equipment.
- Enable independent conformance testing, giving further credibility to the previous two items.

4.9.1 What's Next for 802.16

- Complete the 2 – 11 GHz work.
- Enhance the 10 – 66 GHz specifications:
  - Interoperability test protocols.
- Complete the 802.16c and the 802.16d interoperability testing projects.
- Complete the PICS and test protocols (P1802.16.1, P1802.16.2).
- New enhancements (initiated):
  - Mobility, repeaters, etc.
- Build a basis for 4G wireless.

An update on the latest plans and developments related to 802.16 can be found on the IEEE WirelessMAN web site.[8,9]

4.9.2 802.16 Commercial Products

Given that the 802.16 standard is so new, and in some bands (e.g. 2 – 11 GHz) is still under development and may experience further changes, very few products (if any) exist that can claim to be fully 802.16 compliant. Most commercial products that were found claim some partial compliance, or have plans to migrate to become compliant in the future.

Annex B provides a short description of some of these systems (the list is not exhaustive, but presents a few examples of systems and sub-systems that plan to be compatible with 802.16-2001 or 802.16a).

Some manufacturers also plan to migrate their 802.11a products to support the 802.16a standard.

4.9.3 Security and Encryption in 802.16

In both 802.16 and 802.16a, the MAC layer contains a separate Security Sublayer that provides authentication, secure key exchange, and encryption. For the purpose of privacy, there are two component protocols:

- An encapsulation protocol for encrypting packet data across the fixed broadband wireless access network.

[8] IEEE 802.16 Project Development Milestones: http://ieee802.org/16/milestones.html

[9] IEEE 802.16 Published Standards and Drafts: http://ieee802.org/16/published.html

- A key management protocol (Privacy Key Management, or "PKM") providing the secure distribution of keying data from the Base Station (BS) to the Subscriber Stations (SSs). Through this key management protocol, SS and BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

Overall, security and privacy n the 802.16 can be summarized as follow:

- Secure over-the-air transmissions.
- Protocol descends from BPI+ (from DOCSIS).
- Designed to allow new/multiple encryption algorithms.
- Authentication:
  - X.509 certificates with RSA;
  - Strong authentication of SSs (prevents theft of service); and
  - Prevents cloning.
- Data encryption:
  - Currently 56-bit DES in CBC (cypher block chaining) mode; and
  - Initialization Vector (IV) based on frame number.
- Message authentication:
  - Most important MAC management messages authenticated with one-way hashing (HMAC with SHA-1).

Hence, it can be seen that many security issues have been addressed in the 802.16 standard. Although this security implementation may be sufficient to provide privacy in commercial networks, it does not address some of the requirements needed to make this communications systems a robust military system. This is discussed further in the conclusion below.

4.10 CONCLUSIONS

The use of a commercial technology for military applications should not be based strictly on its known vulnerabilities. These vulnerabilities can sometimes be overcome with additional measures. It should also be considered that given enough time, almost any potential attackers will be able to find holes in most systems. The anticipated tactical use of a communications system must be the main consideration when determining whether the benefits of such a system outweigh the risks associated with the vulnerabilities. Rather than attempting to acquire the perfect system, which most likely does not exist, it is the program manager's responsibility to acquire one that meets the requirements, as required by the operational environment.

With this frame of reference, it is worthwhile undertaking to try to evaluate the impact of the WMAN potential vulnerabilities on the entire communication network. Because the WMAN is based on the 802.16 standard, which only defines operations at the physical and MAC layers, the vulnerabilities explored below are restricted to those two levels.

4.10.1 Physical Layer

There should be little question that the 802.16 standard physical level is highly vulnerable to signal detection and interruption. A commercial standard designed to meet a country's spectrum administration regulatory restrictions and designed to minimize interference will most likely produce, by military standards, a non-robust (vulnerable) signal that could be a significant liability in many tactical situations. Traditional EW techniques of detection, direction finding (DF), and jamming of such a non-robust signal should prove effective and within the capabilities of almost any conceivable adversary. Certain measures can be taken to modify the physical layer of commercial systems, but their effects may be minimal unless major redesign is done. A major redesign would result in a non-commercial, more expensive system, which may have few advantages compared to a system designed from the start for military applications.

4.10.2 MAC Layer

As was seen recently for the 802.11, through a very public debate, MAC layer weaknesses related to inadequate authentication techniques and the use of the WEP protocol showed that this standard was inadequate in providing basic privacy to the users. Although such weaknesses should undoubtedly be a concern in a tactical environment, these weaknesses are more easily correctable than the physical layer vulnerabilities. For example, higher level security protocols and procedures can be implemented or added to the standard to minimize the extent of the MAC compromise.

The 802.16 addresses many of the MAC layer weaknesses discovered in previous standards such as the 802.11, and the design is more robust. It is also more flexible and it allows the use of new/multiple encryption algorithms. Authentication, data encryption and secure over the air transmission provided by the 802.16 may be adequate to protect privacy for the commercial users, but it still does not fully implement the level of security and encryption required by most defense organizations. Adding additional measures of protection on top of the ones provided may reach this goal. It should be noted that the prime motivation for the private sector is the desire for more throughput and low costs, certainly not security at a level as the one required for military operations.

4.10.3 General Conclusions

Many military organizations around the world are experimenting with COTS-based wireless networks to support the next generation of operational concepts which put great emphasis on information superiority. It must be anticipated that a potential adversary will be well prepared with sufficient EW systems and a good understanding of the underlying technology. We could therefore expect to see a resurgence of traditional EW systems, capable of signal detection, DF, and communications jamming. Given this inevitability, it is imperative that a robust RF signal, displaying low probability of detection (LPD) and anti-jam characteristics be employed to ensure the units that will carry out military operation have a reliable means of communications to enable dominant maneuver in the battlefield. With this factor in mind, the impact of the MAC layer security vulnerabilities appears small compared to those of the physical layer.

Some applications that require less advanced capabilities or those that may be conducted in a secure restricted (limited and controlled) physical environment, may well take advantages of COTS systems such as the 802.16. On the other hand, reliable communications in any difficult environment that must go undetected and undisturbed will not be satisfied by this commercial standard. There may also be additional military requirements that need to be implemented and that do not always have their equivalent in the commercial world. An example is the feature of being able to destroy remotely a terminal should it fall into enemy hands.

Notwithstanding the physical layer robustness issues described above, given that the 802.16 is a new, unproven standard, it is also recommended at this time to wait until its widespread deployment before considering it further for military applications. As we have seen with the 802.11 standard, the first and second generations of the standard implementations contained a number of weaknesses that are only now being corrected (e.g. WEP) by issuing new standards (e.g. 802.11g). Hence, given the limited availability of commercial systems that supports 802.16, the real weaknesses of 802.16 are expected to surface only later, when these systems become widely deployed, and when they are subjected to greater exposure and become the target of hackers. Additional difficulties may also surface with the optional use of the Mesh configuration in 802.16a.

Finally, additional characteristics/limitations and issues that may have to be considered when evaluating the use of a commercial wireless standard such as the 802.16 include:

- The use of the wireless devices in one country may not be approved for use in another country, since each country allocates its frequency resources differently.
- Wireless MANs are susceptible to interference, interception, and can be jammed.
- Wireless MANs may create backdoors into military LANs; also, the various wireless and wired interconnection capabilities of WMAN devices present a significant risk that classified information will be compromised over an unclassified medium.
- Those implementing wireless MANs must investigate additional security measures for data confidentiality and network intrusion protection, such as the use of Virtual Private Network (VPN) gateways.
- Administrator must ensure that the users cannot enter a wireless MAN without strong authentication. As a minimum, strong authentication should include extended service set identifier (ESSID) and a media access control (MAC) address identification with an integrity lock. MAC address resolution alone does not quality as strong authentication.
- Multiple wireless transmission-multiplexing techniques are used in the commercial world. Each transmission standard is incompatible with the others. Equipment operating using one standard cannot communicate with equipment using a different standard.
- Where wireless MANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information intercept/monitoring and network intrusion.
- All users must be provided security awareness training regarding the physical and information security vulnerabilities of the wireless devices.

Chapter 5 – WIRELESS PERSONAL AREA NETWORKS (WPANs)

5.1 AN ELABORATION OF THE MULTISPHERE REFERENCE MODEL

The Book of Visions 2000 attempts to propose a reference model, so called the MultiSphere model. Based on the issues and ideas mentioned therein, we present here a more detailed level in terms of functionality and then technologies involved. This is in line with the horizontalisation introduced by 3G's mobile Internet, whereby future vertical applications and services will draw together a multitude of wireless technologies in an ad-hoc manner. In the following paragraphs some of the various spheres of the MultiSphere model are identified. Those addressing general market and commercial needs are omitted and emphasis is placed on the lower, communication related layers.

The technological choices described here aim primarily at a user-centric WPAN, cantered around the person (soldier). This consists (with decreasing emphasis) of his wearable and portable equipment, his immediate neighborhood and his ability to communicate with the wider environment via larger area (wired or wireless) backbones. As a first step we derive corresponding preliminary communications needs. The Book of Visions describes three typical situations: the smart healthy home, the professional environment and the fancy futuristic multimedia traveler. Corresponding environment for military applications have to be considered. It is expected that in both civilian and military environment end-to-end networking with security are the most important concerns, with the additional constraint that the system could comprise a lot of devices.

Except from the general considerations mentioned above there is a number of important and widely employed standards and protocols, either of a generic nature, or particularly adapted to specific application environment. Therefore a survey of recommendations and standards from IEEE 802.15 are attached (see below).

5.2 THE "SPHERES OF THE MODEL"

Communication occurs in three different spaces or spheres: the space that is centered on the person itself, the "outer" local space and the "outer" distant space. These three different spaces translate themselves in three different possible networks: the Personal Area Network (PAN), the Community Area Network (CAN) and the Wide Area Network (WAN).

User requirements of a user-centric Wireless Personal Area Network (WPAN) start from general application scenarios and preliminary communications needs arising from these scenarios. The professional environment, the fancy futuristic multimedia traveler and the combat soldier case, taken as rough first steps call for scalability and end-to-end networking with security. The WPAN, or several WPANs in proximity, could comprise a lot of devices. In the military environment the set of possible devices is also open ended in terms of functionality and scope. So there is a need for scalability in terms of numbers, but also for flexibility to accommodate an open ended set of application possibilities. Finally low-power and possibly low-cost should also be primary design goals for WPAN-based systems and their successful deployment.

5.3 MULTISPHERE LEVEL 1 – THE PAN

In the MultiSphere Level 1 consisting of the PAN, the closest interaction with the Wireless World will happen with the elements that are the nearest to the person or might even be part of his body.

Communication facilities will be contained in clothes, wearable items and equipment carried on a semi permanent basis. We should imagine these devices as starting to discover each other and constituting (spontaneously or at user request) a common virtual terminal the person.

5.3.1 WPAN Devices and Data Rates

At this level Devices and Data Rates have to be considered. This is different from the following spheres presented below, where more "traditional" terminals are to be accommodated in the usual way.

WPAN devices are assumed be in a range from very low power devices with very low communication possibilities to high-end devices covering the full range of communication standards. Low rate devices, e.g. sensors, will have a rate in the range of bits/s while a high rate is considered to be in the range of 10 Mbits/s.

To address this wide range of data rates, two basic options are possible:

- Different physical layers (e.g. 2 or 3), where each address a data rate range (for example 10 bps to 10 Kbps and 10 Kbps to 10 Mbps); and
- Scalable physical layers (data rates, power and cost at least).

Clearly, certain devices will be more capable and costly than others. Simple personal devices (e.g. sensors) must be very low cost and certain less capable devices may even be throw-away. Other more capable devices may incorporate bridge, router or even gateway functionalities, as required to support advanced networking features (see below) and more traditional environments (tactical radios sets, civilian mobile devices, etc.). Relative to other wireless technologies, the WPAN approach should be inherently low cost, due to a scalable and hierarchical architecture and (possibly multiple) air interface options tailored to the service class.

5.3.2 Meshed Nodes with Hierarchy within the WPAN

In the simplest case, the PAN may be a stand-alone network capable of operation independently from other networks. Still, due to the very large range in data rates, it might be useful to put some hierarchy in this simple network by separating the low rate devices from the high rate devices. Hence the need to concentrate several low end devices around a "Virtual Device".

5.3.2.1 The Virtual Device

A Virtual Device is made of two types of devices: Slave Terminals (STs) that can be very simple telemonitoring sensors or actuators and a Master (M). Indeed, as the distance between these devices is short (about 2 meters for a person) and as the use of direct communication between the STs does not appear to be mandatory, the natural topology is a star topology. Hence, there needs to be a Master (M) that co-ordinates the communications and can serve as a display/control terminal. The whole "network" acts as a concentrator from low data rate to higher data rate through the master and can be seen as virtual device from high rate PAN network.

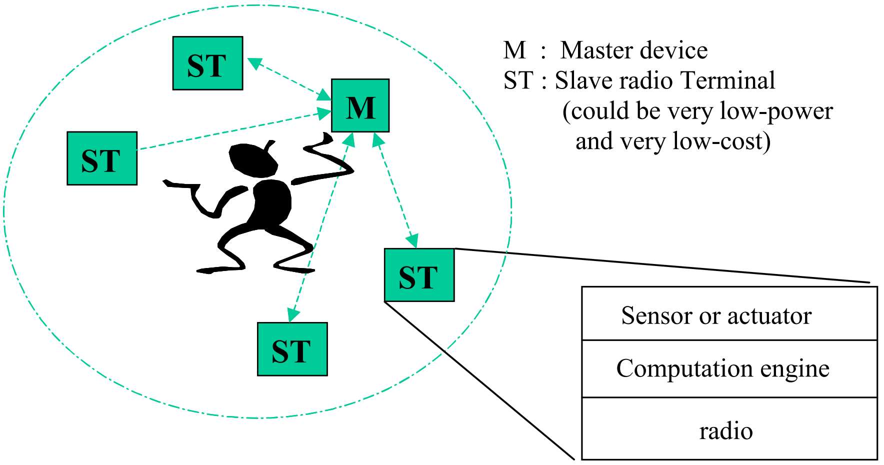


Figure 5-1: The Virtual Device (VD): A Small Standalone Network – A Master with its Accompanying Slave Terminals.

5.3.2.2 The WPAN Consisting of Virtual Devices

Apart from small sensors, a person could also carry a camera, a display (e.g. virtual glasses on which you can see an electronic display), or even more data oriented devices (e.g. computer, keyboard, or printer, weapons with data interfaces). To accommodate higher data rate without wasting bandwidth by duplicating the communications (which would occur if the data going from the camera to the display has to go through the master), the natural topology here is a meshed network (hopefully fully connected, but this can not be guaranteed). Hence, the global picture of a PAN is a meshed network where one of the nodes is a Virtual Device, regrouping the low data rate devices and the other nodes are "advanced Terminals" (aT) (Figure 5-2). Note that dynamic reconfiguration of the network and security issues are less crucial and complex at this level than for the CAN or WAN (see below).

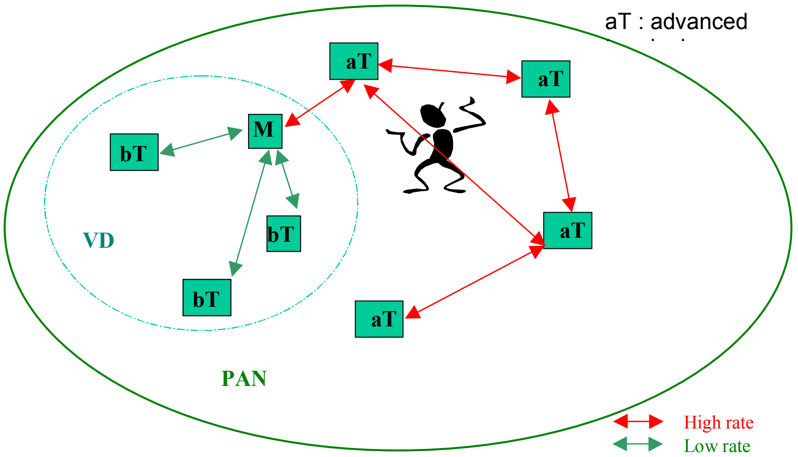


Figure 5-2: The Personal Area Network: A Network of Terminals.

5.4 MULTISPHERE LEVELS 3 & 4: INSTANT PARTNERS

The Book of Visions 2000 addresses here interaction with devices in the immediate PAN environment activated by sensing the physical proximity. This level is here omitted on two ground:

- It can be incorporated within the lower one above; and
- It has reduced military relevance, since these devices are in the civilian case supposed to be "friendly" devices, already programmed for this cooperative behavior. Such an assumption could not be maintained in the military environment case.

5.5 MULTISPHERE LEVEL 5 (INTERCONNECTIVITY) – THE CAN

Next comes the ability to offer advanced networking functionalities and information services through ad-hoc networking, which is the ability to form networks anytime, anywhere, while maintaining the integrity of the information and applications within an individual personal area space. To support ad-hoc networking, the network must be made of bridges (B) (devices that can handle the Layer 2 in the OSI taxonomy) and routers (R) (devices that can handle the Layer 3 in the OSI taxonomy). Community Area Networks (CANs) are formed between two or more PANs, or equivalent network entities The CAN network in itself will be a meshed network and, to enable compatibility with most of the other networks, should be seen as a packet-based IP network. Network elements may be static or mobile. Figure 5-3 provides an illustration.

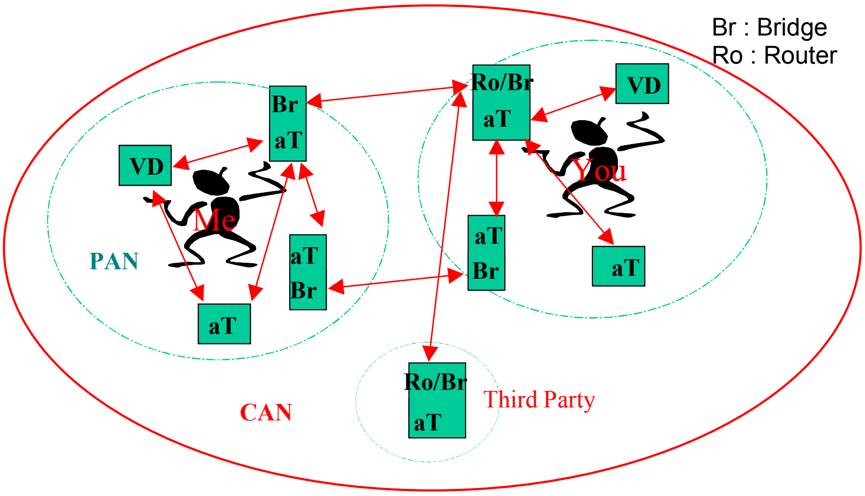


Figure 5-3: The Community Area Network: A Local Network of PANs.

In the wider CAN context, the user's WPAN becomes a private, virtual domain. The capabilities of the user's WPAN may be tailored to support a range of services and quality-of-service (QoS) requirements and scaled in accordance with the available resources per service class and adapted to the prevailing networking capabilities. Tailoring WPAN capabilities includes adaptation to the available resources and downloadable software radio interfaces (i.e. for more capable devices) as well as enhancement of a basic handset or PDA with new software or services, which means that reconfigurable hardware and hardware/software partitioning should be provided.

5.5.1 Gate Keeping Functionality – Security Considerations

Moreover, a person will certainly want to control his privacy and need a gatekeeper to take care of it. This gatekeeper functionality can be tackled by security mechanisms that already exist in, for example, Internet networks. Still, the gatekeeper functionality could be concentrated on one device, or totally distributed among the terminals. A lot of these mechanisms could be borrowed to the existing security schemes. The role of certificate based authentication has to be examined in detail in this context.

5.6 THIRD LEVEL: THE WIDE AREA NETWORK (WAN)

Beyond the WPAN such an envisaged system has to provide global communication possibilities to the user, which calls for the use of classical Wide Area Network systems (mainly, but not necessarily wireless). To enable this, the communications go through a Gateway over these systems (Figure 5-4). Central issues that arise here are security and end-to-end QoS.

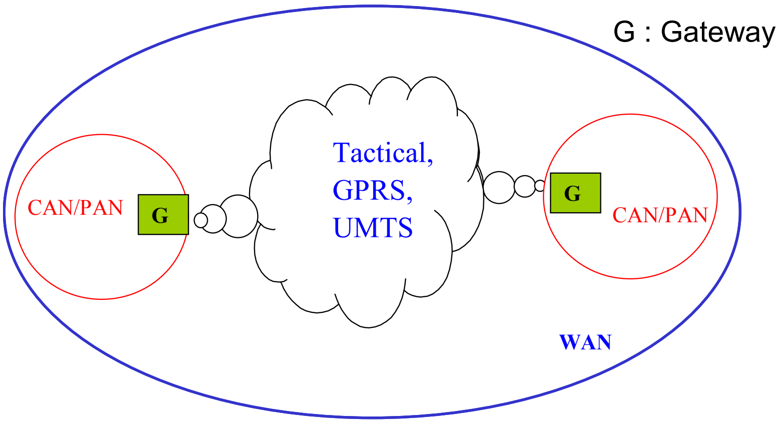


Figure 5-4: The Wide Area Networks (WANs) – PANs/CANs Communicating through External Networks.

Here we have the possibility to rely on ubiquitous coverage of a wide area systems, either directly from the PAN or via the interconnection possibilities offered at CAN level. Adaptivity to various terminals and simple inter-action with the backbone are key issues.

5.7 MULTISPHERE LEVEL 6: CYBERWORLD

According to the MultiSphere Level 6, the outmost sphere, most remote from the immediate real world, represents the CyberWorld. In the CyberWorld one can in touch with (semantic) agents, knowledge bases, communities, services and transactions.

The value of communications technologies is sometimes said to grow proportionally to the square of the number of the connected devices. Therefore, it will be a crucial task to maintain universal wireless interconnectivity, as in today's mobile Internet core networks. To offer the right level of support for the various specialised radio interfaces and terminals will be a key requirement. One can therefore see an emerging need for both a radio convergence layer and a number of APIs beside the evolved IP transport and networking layers. Evolutions of interconnectivity in the Wireless World will convey radio interface state specific information to applications and also allow for seamless integration of synchronous direct communication services with asynchronous message based services.

5.8 OVERVIEW OF RELEVANT STANDARDS

5.8.1 IEEE 802.15

The IEEE 802.15 is the IEEE working group for Wireless Personal Area Networks (WPANS) and is developing standards for Personal Area Networks or short distance wireless networks. Established in January 1999, the WPAN working group, which is part of the Local and Metropolitan Area Network Standards Committee of IEEE, has since formed four task groups, each work on necessary standards.

The idea of WPAN is to create standards that allow devices such as PCs, PDAs, mobile phones, pagers, and other handheld devices to communicate and collaborate with one another. Unlike LAN devices, which are fixed, WPAN devices will travel and transfer. This means that the same standard should work everywhere, in a car, on a boat or a plane, and in different countries. Also, in our days people expect some synchronous services, at least voice, to be provided apart from data applications.

Those familiar with Bluetooth will recognize that these are some of the same considerations that are handled by Bluetooth. The WPAN standardization effort started at least a year before the public announcement of the Bluetooth standard. The goal of the 802.15 standards is to accommodate wider adoption and applicability. The main characteristics of a WPAN are:

- Low cost,
- Low power,
- Short-range,
- Small networks.

5.8.2 Architecture of the 802.15 and Relation with Bluetooth

The IEEE 802 Standards Committee is primarily focused on the layers 1 and 2 (Physical and Data Link) of the Open System Interconnection (OSI) Reference Model. The 802.15 WPAN is one of the IEEE series of standards that falls under the 802 standard. The 802.15 WPAN committee is working on standardizing the PHY and MAC layers of Bluetooth. Below is the architecture of the 802 standard illustrating where the focus of the standard is in relation to the OSI Reference Model and how it relates to Bluetooth:

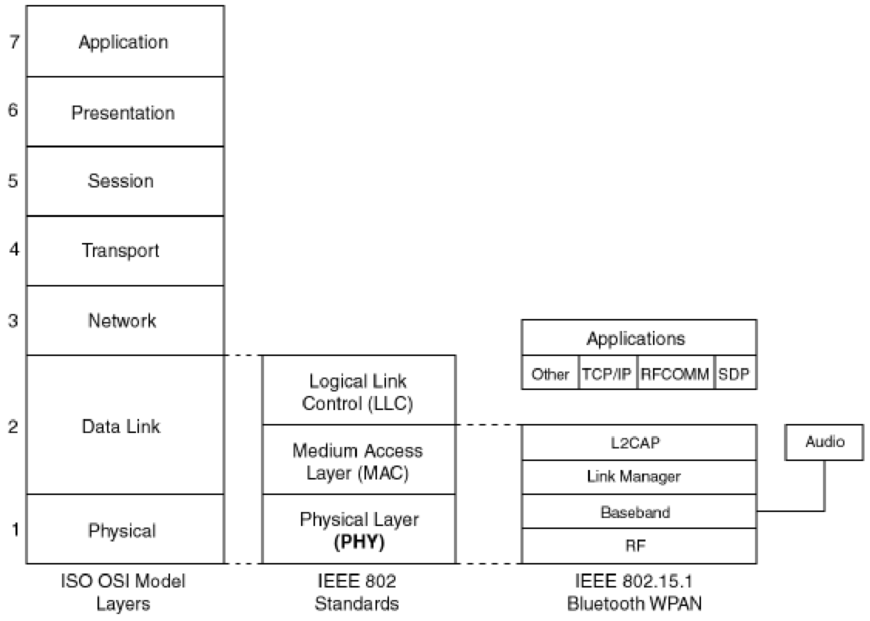


Figure 5-5: IEEE 802.15.1 Protocol Stack.

5.8.3 (UWB) 802.15.3a – Main Characteristics

In Ultra Wide Band (UWB), pulse modulation involving extremely short bursts of RF occur. A typical pulse can be in the order of 0.1 to 2 nsec with resulting emission bandwidth of GHz heavily depending on the rise time of the leading edge as well as on the antenna pass band. The spectrum spread in extremely high in the order of 25% of the center frequency, which also makes UWB signals very difficult to detect.

Besides the razor thin rise time, the precise timing of UWB pulses can be employed in communication (pulse position modulation) as well as in radar applications (soil penetration radars, seeing and positioning through walls, etc.). Also indoors localization via triangulation methods is another promising area of applications.

UWB is excelling in spatial capacity, measured in kilobits per second per square meter (kbps/m2). Spatial capacity focuses not on bit rates for data transfer alone, but on bit rates available in the confined spaces defined by short transmission ranges. Thus the extremely low power to be used in UWB in the context of WPANs (Wireless Personal Area Network – WPAN) ensures extremely high bandwidth at very low range (few meters) and power. It thus achieves very high spatial capacity.

UWB is expected to become the solution adopted in the 802.15.3a IEEE standard and corresponding regulatory activities are now well advanced. FCC has given qualified approval to UWB usage, following nearly two years of commentary by interested parties. Issues like UWB interference with existing services such as GPS, radar and defense communications and cell-phone services have been considered. UWB communications are allowed for applications with full "incidental radiation" power limits of between 3.1 and 10.6 GHz. Outside that band, signals must be attenuated by 12 decibels (dB), with 34 dB of attenuation required in areas near the GPS-frequency bands. More liberal restrictions were permitted for law-enforcement and public safety personnel using UWB units to search for earthquake or terrorist attack victims.

5.9 SECURITY REQUIREMENTS

The security requirements for 802.15 networks are different from more static networks because of the dynamic nature of wireless PANs. As a result, the working group is looking into specifying public-key solutions for authentication and key exchange, letting devices that have not been in contact previously establish secure communications without revealing any secret keying material.

Once the devices have been authenticated, each device in the wireless PAN shares common group (symmetric) payload protection keys for encryption and data integrity. Devices also may use the authentication mechanism to establish two-party secure subnetworks. This procedure is similar to this for establishing an SSL connection between a server and a client.

5.10 FUNCTIONS OF LOWER LAYER PROTOCOLS

5.10.1 RF Layer

The air interface is based on antenna power range starting from 0 dBm up to 20 dBm. Bluetooth operates in the 2.4 GHz band and the link range is anywhere from 10 centimeters to 10 meters.

5.10.2 Baseband Layer

The Baseband layer establishes the Bluetooth physical link between devices to make up a piconet. A piconet is an ad-hoc network of devices using Bluetooth technology. A piconet is created when two Bluetooth devices connect, and it can support up to eight devices. In a piconet one device acts as the master and the other devices as slaves.

5.10.3 Link Manager

The link manager sets up the link between Bluetooth devices. Other functions of the link manager include security, negotiation of Baseband packet sizes, power mode and duty cycle control of the Bluetooth device, and the connection states of a Bluetooth device in a piconet.

5.10.4 Logical Link Control and Adaptation Protocol (L2CAP)

This layer provides the upper layer protocols with connectionless and connection-oriented services. The services provided by this layer include protocol multiplexing capability, segmentation and reassembly of packets, and group abstractions.

5.10.5 Differences of the WPAN (802.15) from the WLAN (802.11)

A wireless local area network (802.11), uses high-frequency radio waves instead of wires to communicate between nodes in a network. Wireless personal area networks differ from wireless local area networks at the interaction, packet format, type of devices, network build-out timeframe, relative cost, and general network architecture. The Wireless personal area network concerns highly mobile devices; it is cheaper and consumes less power.

5.10.6 802.15 WPAN Task Group 1

The 802.15 WPAN Task Group 1 (TG1) is using the Bluetooth v1.0 specifications to derive the WPAN standard. The scope and focus of TG1 are to define PHY and MAC specifications for wireless connectivity between devices that are either fixed or portable within the personal operating space. The goal will be to allow low complexity, low power consumption wireless connectivity to support data transfer to and from a WPAN device and an 802.11 device. The proposed standard will take into account coexistence with all 802.11 devices.

5.10.7 802.15 WPAN Task Group 2

Task Group 2's (TG2) scope and focus is to address the coexistence of WPANs and WLANs. TG2 is developing a coexistence model to quantify the mutual interference of a WLAN and a WPAN. The Task Group is also developing a set of coexistence mechanisms to facilitate coexistence of WLAN and WPAN devices.

5.10.8 802.15 WPAN Task Group 3

Task Group 3's (TG3) scope and focus is to publish a new standard for a high data rate, 20 Mbps or greater, for WPANs. TG3 will also be looking at providing a solution that is low power and low cost, addressing the needs of digital imaging and multimedia applications. The new standard will comply with the TG1 standard.

5.10.9 802.15 WPAN Task Group 4

Task Group 4's (TG4) scope and focus is to determine a solution with a low data rate and long battery life, potentially months to years, with very low complexity. The solution determined would need to operate within an unlicensed and global frequency band. The solution could potentially be applied to sensors, remote controls, appliances, toys, etc.

5.11 REFERENCES

- http://www.ee.iitb.ernet.in/uma/~aman/bluetooth/tut6.html
- http://www-106.ibm.com/developerworks/library/wi-checking/?dwzone=wireless
- http://www.nwfusion.com/news/tech/2002/0311tech.html
- WWRF, "Book of Visions Parameters" based on the devices and communications of the scenarios.

The following table lists the most significant devices of relevance to WPANs together with corresponding requirements in relation to the communications that these devices will need.

Table 5-1: PAN Specifications

Devices	Information Rate	BER needed for the application	Latency (End-to-end, possibly IP)	Power	Range	Size/Weight	Autonomy	Mobility/ Speed	Price
Virtual Glasses + headset	8 kbits/s (terminal) 500 kbits/s (MPEG4 – VHS quality) 10 Mbits/s (MPEG2 – HDTV quality)	10^{-3} FER : possible for MPEG-4 10^{-7} for MPEG-2 at MAC-layer (MPEG -2 asks for error-free transmission)	< 150 *ms* preferred <400 *ms* limit Lip-synch: < 100 *ms* [1] for fixed images or one way streaming: <10 sec	Today 4 or 18 watts ? 100 mW for the visual part bet on < 1 W 5 Mbits/s with picoradios 5 nJ/bit : 25 mW radio + MPEG : 250 mW for UMTS videophone chip .25 um chip (JVLSI 2000) + 100 mW visual → 250 mW	2 m for Master 10 m for Bridge	100 to 250 gr virtually invisible	1 day → 2 days	Low mobility (< 0.5 m/sec) for movie Medium mobility (< 3 m/sec) for terminal/sound type	Target 100 $ (Sony wired 18 W : 600 $) MPEG 2-coder/decoder about 100 Kgates
Video camera	10 kbits/s for non-real time still images 500 kbits/s (MPEG 4 – VHS quality) 10 Mbits/s (MPEG2 – HDTV quality) (depends on the local intelligence)	Not applicable (N/A)	N/A coding	Same as above for radio: 25 mW Camera?	2 m for BT 10 m bridge	100 gr	2h → 2 days	Low mobility (< 0.5 m/sec) for movie Medium mobility (< 3 m/sec) for still image	Target price 10 $
Plain headset	8- kbits/s up to 1.4 Mbits/s (HiFi) MP3: <250 kbits/s HiFi	10^{-3} (toll-quality+ intelligence)	For conversation : < 100 *ms*	Radio < 10 mW (aim 1 mW) Sound: 20 mW (verify) Coding ?	2 m for BT 10 m for bridge	25 – 50 gr	Minimum 1 day up to 1 month	Medium mobility (< 3 m/sec)	Target price for the radio 1$ (low quality headset 5 $)

[1] Taken from 3gpp specs : 3G TS 22.105 V4.1.0 (2001-01).

Devices	Information Rate	BER needed for the application	Latency (End-to-end, possibly IP)	Power	Range	Size/Weight	Autonomy	Mobility/ Speed	Price
Wireless microphone	8 to 64 kbits/s	N/A	Coding latency ?	ALAP Coding ? Radio < 1 mW (otherwise it should be on the M-WAP)	2 m for BT 10 m for bridge 10 m for me to you (hearing aid)	10 gr	Minimum 1 day up to 1 month	Medium mobility (< 3 m/sec)	Target price : very low (< .5 $)
Translation device (probably in the M-WAP)	8 to 64 kbits/s (x2)	10^{-3} (toll-quality+ intelligence)	1 sec for the radio	For the radio: 1 – 2 mW	2 m for BT 10 m for bridge	To be determined	To be determined	To be determined	Target price for the radio 1$
Sensors (passive : tags)	< 1 kbits/s	Service dependent	< 1 sec	100 uW 1 mW 10 mW	2 m for BT 10 m for bridge	1 – 10 gr	Up to 1 Year for the low power	Low mobility	For the radio 10 – 20 cents Other < 1$
Joysticks (power can come from force)	Up to 1 kbits/sec	To be determined	< 10 *ms*	Radio < 1 mW	2 m for BT 10 m for bridge	To be determined	To be determined	To be determined	Target price for the radio 1$

5.12 PAN IN THE CONTEXT OF WIRELESS TECHNOLOGIES STANDARDS

The table bellow shows the relationship between established wireless technologies standards and the PAN approach, as described above. Main points to be emphasized are (i) the split into PAN and CAN which brings the need of a wide range of supporting wireless technologies (in terms of range, speed, mobility, bandwidth) and (ii) the possibility to realize the PAN/CAN approach by employing upcoming standards and maturing technologies.

Table 5-2: Comparison of PAN with other Technologies

	802.11a	802.11b	802.15	Homerf	Bluetooth	Infrared (IrDA)	Personal Area Network	
							PAN	CAN
Speed	0.5 m/s	0.5 m/s	0.5 m/s	0 m/s	0.5 m/s	0 m/s	0.5 m/s	3 m/s
Mobility Support	Micro-mobility support	Micro-mobility support	Micro-mobility support	No mobility support	No-mobility support	No-mobility support	No-mobility support	Full-mobility support (QoS handover, distributed resource management)
Market	Wireless Local Area Network (WLAN)	Wireless Local Area Network (WLAN)	Wireless Personal Area Network (WPAN)	Wireless Local Area Network (WLAN)	Wireless Personal Area Network (WPAN)	Wireless Personal Area Network (WPAN)	Wireless Personal Area Network (WPAN)	Mobile ad-hoc Network
Technology	Radio Frequency 5 GHz, OFDM	Radio Frequency 2.4 GHz, FHSS, DSSS	Radio Frequency 2.4 GHz, FHSS, QPSK, QAM16	Radio Frequency 2.4 GHz, FHSS	Radio Frequency 2.4 GHz FHSS	Optical 850 nm	Wider frequencies and channels	Wider frequencies and channels different than in PAN
Transmit Power	1 Watt	Moderate 100 mW	.5 .. 4 mW	100 mW	Low 1 – 100 mW		.1 mW	1 – 100 mW
Data Rate	High 54 Mbits/s	High 2 / 11 Mbits/s	Low / High up to 41 Mbits/s	0.8 and 1.6 Mbits/s	Moderate 1 Mbits/s	Low 115 kbits/s / 4 Mbits/s	Low…High 1 kbits/s … 10 Mbits/s	Low…High 1 kbits/s … 10 Mbits/s
Distance		30 meters / 98 feet	10 meters (20 Mbits/s) / 5 meters (41 Mbits/s)	50 m	10 meters / 32 fee	5 meters / 16 feet	2 m	2 m – 10 m
Topology	128 devices CSMA (?)	128 devices CSMA	10 devices point-to-multi-point	128 devices CSMA/ CA+TDMA	8 devices point-to-multi-point	10 devices point-to-multi-point	10 – 30 BT	Infinite … 1 – 5 RGB/m2 30 BT/m2
Security	??	Optional WEP	Public/Private key authentication and encryption	56 bit shared key encryption	Public/Private key authentication and encryption	Application Layer		Layered security, firewalls, application

Chapter 6 – COMMAND POST AND URBAN OPERATIONS

To be able to follow operations closely, future command posts will be even more mobile than they are today, at least at lower echelons (below division level). In order to achieve high mobility, command posts will be installed on mobile platforms (vehicles etc.). As the number of personnel might be too high for a single platform, a command post may be dispersed on a number of platforms. In addition, this reduces the vulnerability and increases the survivability of the command post.

The requirement for communication within the command post (between the platforms) will be for all services (voice, data and video) with a demand for high capacity (analogous to that of a LAN). The command posts may have to operate in vegetated terrain or in urban areas where direct line-of-sight between the platforms will be difficult to achieve. For those command posts with the highest mobility, this means that the communication system should not rely on frequencies above UHF in order to achieve a reasonable availability without the need to consider communications when locating. For command posts with a lower degree of mobility the need for communications capacity may exceed the freedom of positioning. This will allow the use of higher frequencies that require LOS. All communication systems should also offer automatic relaying of packet-switched information.

For urban operations there will always be a question of bringing own communications equipment to build an infrastructure or to use existing communications infrastructure. Even though cellular phone systems and wireless LANs will be extended to even quite remote and poorly developed countries in the near future, few commanders will be willing to rely on such an uncontrollable infrastructure for military operations (maybe with the exception of purely peacekeeping operations). This means that for most operations the armed forces will have to bring their own communications infrastructure – operational from day one.

Urban operations may be much more challenging with regard to communications than operations in rural areas. Tall buildings, often constituted by reinforced concrete or covered with metallic plates will not only attenuate radio signals, but also increase the problem of multipath propagation and signal fading. Future military communications should address the problem of multipath, utilizing different techniques to combat this problem. There is also the problem of operations under ground, in basements, parking houses and subways and other tunnels. In this situation, reliable communication will be a real challenge. Possible solutions are the use of small, automatic repeaters.

There are two different strategies for the communications network architecture:

1) Ad-hoc networks not requiring a base station infrastructure to be operational. Mobile units may communicate directly between each other, or by the aid of any other mobile. Traditional Combat Net Radio (CNR), Military Packet Radio and Wireless LAN (in ad-hoc mode) are typical representatives for this kind of architecture.

2) Networks relying on an extensive infrastructure. In this kind of network two mobiles are unable to communicate unless both are connected to the infrastructure. All communication usually is relayed by the infrastructure, even though the mobiles are within radio range.

Both for command post and urban operations there will be a need for two different kinds of communications:

- Intra-network communication within and possibly between the units deployed in the area of operations; and

- Inter-network communications between geographically separated areas of operations and communications “back home”.

These two different communications needs will probably require quite different solutions as the latter is often met by satellite communications while the first is probably best met by ad-hoc radio communications.

To reduce the cost of procurement and in order to be able to exploit the rapid evolution of the commercial telecommunications market, there might be a desire to use commercial equipment to a large extent, or at least to use equipment based on commercial standards and components. This should not be done without a critical mind. Commercial systems and components are not always made with military requirements in mind, and may not always be suites for such operations. At least, special consideration should be taken in order to ensure that all aspects and properties are evaluated against the military requirements and that the risk is considered to be reasonable for the current operation.

Unlike commercial systems, military communication systems should not rely on qualified technical personnel to be available to manage and repair the system. A high degree of automation should be build into the system, as the users may not be expected to be experts on communications.

Chapter 7 – SOLDIER NETWORK

In the near future, even the individual dismounted soldier will be connected to the military information grid through a communications network. Although the current requirement for the soldier primarily is for broadcast voice communications, in the future this may be very much shifted to include non real-time data communications as the primary requirement, with telephony and video as secondary requirements. The soldier rarely operates alone, but usually in a group. The group has a requirement for internal communications as well as a communication link to the network. Solutions for communication within the group are not well established and pose challenges with regard to equipment size, weight, power consumption and antenna solutions.

As the soldiers often operate in hostile environments, they must rely on systems based on ad-hoc network architectures. In order to extend the radio range and achieve a higher availability of communications the system should offer automatic routing and relaying of information.

Chapter 8 – MILITARY RELEVANCE: SECURITY, INTERCEPTABILITY, ECM ISSUES

8.1 GENERAL SECURITY ISSUES

Many security issues arise in wireless networks because of the fact that wireless is a shared medium and everything that is transmitted or received over a wireless network can be intercepted. Because of the large range of the transmissions (a few kilometers), the 802.16 signal is particularly vulnerable since it is made available (for interception and detection) to anyone located within this large perimeter.

To secure a mobile wireless network, one must consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

- **Availability** ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of a wireless network. On the physical and media access control (MAC) layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.
- **Confidentiality** (secrecy) ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.
- **Integrity** guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.
- **Authentication** enables a node to validate the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
- Finally, **non-repudiation** ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

Two types of attacks are considered in communications:

- **Passive Attacks** – These types of attacks typically involve eavesdropping of data. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. This also makes defending against such attacks difficult.
- **Active Attacks** – These involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data.

8.2 SECURITY CONSIDERATIONS FOR 802.11

The US standard IEEE 802.11 with its several extensions or versions (indicated by small letters) gives specifications for WLAN systems. A WLAN system is a radio system with a typical range from several ten up to several hundred meters. The main purposes are to connect client-PCs and servers with each other and with peripheral equipment like printers. The necessary bandwidth is generally higher than that of a WPAN system because of the requirements to exchange larger files and to run lavish applications across the network. The nominal data rates reach from 1 Mbps for the older system versions up to 54 Mbps for the newer ones. The maximum allowed transmitter power depends on the region (e.g. Europe or US), the application and the frequency range. EIRP values (Equivalent Isotropically Radiated Power) for indoor applications are typically limited to 100 or 200 mW and for outdoor applications to 1 W.

The 802.11 wireless networks operate in one of two modes, ad-hoc or infrastructure mode. In the ad-hoc mode the network is self organizing its structure and each client is able to communicate directly with the other clients within the network. The ad-hoc mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell must operate as a gateway and perform routing. In infrastructure mode, each client sends all of its communications to a central station or Access Point (AP). The AP is responsible for the synchronization, for energy economy measures and for the multiple access steering in the LAN. The AP acts as an Ethernet bridge and forwards the communications onto the appropriate network, either the wired network, or the wireless network. Roaming between APs is supported.

Above the MAC layer a 802.11 system looks like every other 802.x LAN and provides comparable services, e.g. in connection with the often used wired Ethernet LAN (IEEE 802.3). The mechanisms for the channel access in the MAC layer are the same for all 802.11 versions. The access method is the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). With this method the channel activity is observed and a new transmission is only started, if an appropriate channel is found. In addition, the mobility management is done in the MAC layer. Only slow motion is allowed for the mobile terminals. The transport of information is done in the packet switched mode.

8.3 THE STANDARDS/SYSTEMS

At present, the mostly used system version is the 802.11b, which works in the license-exempt IMS frequency band around 2.4 GHz. It uses PSK modulation types and a DSSS technique with a channel bandwidth of 22 MHz. The nominal data rates are 5.5 and 11 Mbps. The purpose of the DSSS technique with its short code length of 8 chips is to improve the separation against other users in the IMS frequency band and to separate transmitted information bits from each other. The type for the spreading/coding method used here is CCK (Complementary Code Keying). The separation of different channels used in parallel is done with FDMA. The available frequency band reaches from about 2.40 GHz to 2.48 GHz and is divided into fourteen overlapping channels which give the available frequency set pattern. Within this frequency range only three non-overlapping channels each with a width of 22 MHz can be used in parallel. In Europe the parallel use of more than three of such channels is in fact allowed but in these cases there are frequency overlaps.

In the US influenced countries the probably most interesting realization in the future will be the version 802.11a which uses the frequency band around 5 GHz. The development takes care of the regulation concerning the US license-exempt band in this frequency region. This band is exclusively reserved for WLAN applications, other systems like e.g. microwave ovens are not allowed. The nominal data rates reach from 6 up to 54 Mbps. The bandwidth of each channel is 20 MHz and up to 12 non-overlapping channels will be available. The modulation types are PSK with 2 and 4 states and QAM with 16 and 64 states. The modulation type actually used depends on the requested data rate. As the competitive systems in Europe (HIPERLAN II) and Japan (HISWANa: High Speed Wireless Access Network, Version a), IEEE 802.11a uses the OFDM method too. This frequency multiplexing method allows high data rates with comparatively good robustness against frequency diversity disturbances. The use of the today's 802.11a version is not allowed in Europe because it is not fitted to the features DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control). These features are prescribed in Europe and should prevent conflicts with the HIPERLAN II system.

The version 802.11g is comparatively new. The aim is to enable higher data rates in the 2.4 GHz band, at present 22 Mbps. 802.11g shall be backward compatible with 802.11b. For high data rates, OFDM and for the lower data rates CCK shall be used. At present it seems, that the work within this group does not show quick progress. The reason could be, that the development tendency is more directed towards the version 802.11a with its higher available frequency bandwidth and data rates.

The 802.11h standard is the version 802.11a, supplemented by DFS and TPC which are necessary for the use in the European 5 GHz band. DFS seeks the frequency channels with the best availability and TPC minimizes the transmitted power. These features should prevent serious conflicts with HIPERLAN II.

802.11i includes extensions of the MAC protocol with improved mechanisms for security and authentication. The approval is planned for the year 2003.

8.4 INTERCEPTABILITY

The standardized 802.11 parameters of RF frequencies, bandwidths, waveforms, protocol formats and the security mechanisms are well known. In addition, the WLAN principle is not well suited to sophisticated protection measures against interception. Because of the requirement of setting up radio connections in a flexible manner with comparatively cheap equipment, the hurdles for getting network access have to be moderate. On the civil market several tools for monitoring 802.11 radio traffic are offered, partly free of charge. One example is the *Netstumbler* which could be used together with the *Orinoco* WLAN board of Agere Systems. But a monitoring is only possible within comparatively small distances from the network, caused by the mostly low emitted power and the high radio frequencies with their limited transmission range.

There would be perhaps some interception difficulties if some of the elementary parameters of the 802.11 signals/systems were changed. This could have been done with the aim to adapt to specific (e.g. military) requirements. An example could be the choice of a lower radio frequency for extending the transmission range. Other elementary parameters concern the methods of modulation, spreading and multiplexing. To intercept such special systems with unknown parameters, the requirements for an interception receiver concerning bandwidth, dynamic range and speed could be demanding.

The available 802.11 products (802.11b systems) have several protocol security mechanisms, but these mechanisms do not constitute high hurdles for a well equipped interceptor. While overcoming these hurdles, the access to the foreign network opens up several possibilities. The aim of the activities subsequently possible (e.g. intrusion and insertion of falsified information) could go beyond the classical interception tasks (examination of technical characteristics, identification, traffic analysis, message content). Nevertheless most of the weaknesses of the protocol security mechanisms are discussed in this section and not in the next section concerning ECM issues because they concern primarily the interception.

At the lowest level the acceptance of a requesting terminal is regulated by means of an ID number, the ESSID (Electronic System ID). An administrator has entered the ESSIDs into all involved APs and mobile terminals in advance. The ESSID indicates the access entitlement of a terminal but does not allow its unambiguous identification. There are two weaknesses concerning the ESSID: Firstly, it is no problem to find a general access number with the aim to monitor the radio traffic. Secondly, most terminals schedule the option *any* in their configuration file. With this setting the terminal will be allowed to get access to any network.

The authentication mechanisms allow only the entitled terminals to take part in the communication. The checking is done in the Link Level Authentication process between the involved stations. The mechanisms use the MAC addresses of the mobile terminals, which are stored in the AP access list. But it is possible to change the MAC address within most of the available products. Such a manipulated terminal will be allowed to get access to foreign networks. With many of the available products an additional weakness is the awkwardness of the authentication process within larger networks. The consequence may be, that the complex authentication process is not used. In this way the access to such a foreign network would be made easier.

Although the ciphering of the information content could be done by means of the WEP (Wired Equivalent Privacy) protocol, the security of the today's simple version with a key length of 40 bit is limited. WEP uses a static key. If the key is known there is no longer any protection. This concerns not only the data ciphering but also the higher quality authentication protocol because therein WEP is used too. Otherwise, if the key is not known, one has the possibility to observe the traffic for a longer time and to extract important information. Using this information it is possible to compute the key and decipher the information content. The available tools for these tasks are e.g. *Airsnort* and *Wepcrack,* which are offered in the Internet, free of charge. By means of these tools the key could be extracted within a few hours. There are two additionally weaknesses: Firstly, WEP is only an optional system feature, it is not included in the standard. Companies who offer 802.11 conform products are not obliged to offer the WEP protocol. Secondly, products offered from different companies could have different key lengths. This often causes non-interoperability while using WEP. As a consequence, only the simple common WEP protocol is used or WEP is not used at all. In this way the interception would be made easier.

8.5 ESM AND ECM FOR THE IEEE 802.16 STANDARDS

The 802.16 standards provide certain protection measures against signal interception on the MAC layer with possible improvements for satisfying not only commercial but also military use. It also has been mentioned that the main weakness is provided by the physical layer because of its highly vulnerability to signal detection, direction finding, and jamming. This assumption may be based on commercial needs, for example:

- W-MAN radio base stations use antennas with relatively broad sector beams of up to 90° beamwidth for covering as many terminal stations as possible.
- Distances between the base and terminal stations reach from 2 km (at 42 GHz) to 15 km (at 2.4 GHz), dependent on the used frequency band.
- The possible frequency bands are allocated to the user and known to the public.

Under these circumstances it will be possible for an adversary to locate his ESM/ECM equipment within the radio path between the base and the terminal station for detecting the downlink signal and jamming the uplink signal.

However, tactical military applications will not be dependent so much on commercial aspects. That means, military may use measures able to reduce considerably the danger of signal detection by an adversary, which is the pre-condition for effective jamming, for example:

- The radio base stations may have antenna structures of smaller beamwidth, for example 15° or less. For detecting the downlink signal, the ESM equipment needs to be located then more precisely to the radio path.
- The distances between the base and terminal stations may be less than a few km. In this case an adversary will have difficulties to put his ESM equipment within the radio path near the base station. He has to try to detect the more attenuated signal from a place behind a terminal station.

- The base stations may use power control. This function is not yet included in the IEEE 802.16, but in the ETSI standards for Hiperman and Hiperaccess. However, one can assume, that the power control function will be overtaken also from the 802.16 standards. Using the power control function, together with the measures mentioned before, will make it harder for an adversary to detect the downlink signal.
- In difference to commercial providers, who have to use allocated frequency bands publicly known, military may have the choice among a number of frequency bands within the lower frequency range of 2 – 11 GHz (802.16a), or the upper range of 10 – 66 GHz (802.16-2001). Accordingly, an adversary does not know the used frequency bands a priory and has to search for the downlink signal within rather broad frequency ranges. Of course, this task would become still more difficult, if one would change the used frequency band within more or less short periods.
- If one uses the frequencies around 60 GHz for short distances one would have the advantage of, compared to other frequencies in this range, very high propagation attenuation.
- Military may prefer the standard 802.16a for the frequency range 2 – 11 GHz due to the requirement of only near line of sight conditions. This would include the advantage to transmit by OFDM, a technique which is robust against frequency selective disturbances or narrow band jamming.

As mentioned above, effective signal jamming needs to detect the signal before. Of course, a base or terminal station may be jammed by an adversary’s jammer without detecting a signal. But, taking into account the above described measures, it would need much power over a broad frequency range for the jamming signal to obtain sufficient effectiveness, with a high probability of physical destruction of the adversary’s jammer.

For the susceptibility and ESM and ECM for the whole spectrum of IEEE 802.11 series of standards see Chapter 8, specifically devoted to this issue.

8.6 ECM ISSUES

It seems not difficult to jam a whole WLAN network if the jammer could be placed near enough. The comparatively high radio frequencies have limited transmission range. While the nominal ranges are limited to several hundred meters, the application of directional jammer antennas, possibly combined with higher transmitter powers, could extend the range. Smart jamming in kind of intelligent jamming of single terminals is probable of minor importance because of the limited geometrical network extension. An exception would be the case, where the jammer is placed inside of a network, e.g. in a local area mission.

If there exist several (sub-) networks, which are wirelessly connected, it seems easier to place a jammer *between* networks than to place it *inside* a network. The victim connections between the networks will be realized with techniques in agreement with 802.11, 802.16 (WMAN) standards or other directional radio systems for larger distances.

As mentioned in the last section, it is possible to surmount the today’s protocol security mechanisms by means of appropriate tools. The aim could be not only the interception but the intrusion and insertion of falsified information too. This possibility is not only given because of the weaknesses concerning authentication and data ciphering. In addition the specific realization of the CRC mechanism (Cyclic Redundancy Check) is a weakness. This mechanism is used to recognize unintentional data changes during transmission, i. e. the message integrity should be controlled. But the additional checksum bits are attached *after* the information has been ciphered. This gives the possibility to manipulate the information and afterwards adapt the checksum bits. In this way messages may be modified in transit without detection, in violation of the security goals of the provider. The details of such measures belong more to the Information Warfare than to the Electronic Warfare section.

8.7 MILITARY RELEVANCE

The possible use of the today's 802.11 systems for own forces would be limited because of the discussed weaknesses. Nevertheless the system use is conceivable in a limited and well controlled area, e.g. in a non-distributed headquarter. The probability of fraudulent use has to be low.

A disadvantage is the lack of DFS and TPC if several different networks are used in parallel and the network distances are low. Then strong interferences are to be expected.

Another disadvantage of the 802.11b systems could be the minor data rate. Instead of the nominal 5.5 or 11 Mbps the practically reached data rates are at best between 3 and 4 Mbps, also for isolated point to point connections. The version 802.11a with its up to twelve 20 MHz channels will have more capacity.

There are perhaps two militarily interesting development tendencies: a) The recommendations and the further work of several civil groups with the aim to improve important features; and b) The possible change or adaptation of important system parameters to specific (military) requirements. In the following, some items concerning these tendencies are given.

a) Recommendations and further work of civil groups or companies:

- For WLAN participants it is recommended to consequently use the today's offered security mechanisms concerning authentication and ciphering as far as possible. It was found out that in most of the observed WLAN networks the mechanisms were not used because the participants are not really aware of the possibility or probability of fraudulent use.
- It was recommended to use the WLAN in front of a firewall, i.e. the firewall stands protectively in front of the host computer.
- Another recommendation is the application of an IDS (Intrusion Detection System).
- For information in need of protection it is recommended to use the WLAN independent VPN (Virtually Private Network) concept. A VPN is based on the so-called tunneling method, mostly realized in layer 3. The tools used in this context could be IPSEC or PPTP (Point-to-Point Tunneling Protocol). Another known security mechanism is the SSH (Secure Shell).
- Some companies use further developed methods to obtain more authentication security. These methods are combinations of the EAP (Extensible Authentication Protocol) and the suggested standard 802.1X for the controlled Ethernet access. EAP is an extension of the RADIUS (Remote Access Dial-In User Service) with PAP (Pathword Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). With 802.1X the authorized access for larger user groups with wireless and wired terminals can be organized.
- Some companies offered further developed WEP ciphering methods: With the Agere Systems' solution *WEPplus* the generation of the initialization vectors for the ciphering is improved and the susceptibility to AirSnort should be removed. WEPplus is backward compatible with the simple WEP. RSA Data Security Inc. offered a new method called FPK (Fast Packet Keying) with which the code is changed for every new data packet.
- The weaknesses of authentication and ciphering in the today's 802.11 versions are well known and there are official endeavors to improve the mechanisms. The standardization group 802.11i is working on it. One important item is the application of the AES (Advanced Encryption Standard). Before the standardization work will be finished, the group recommends the general use of the

104 bit ciphering key length and the application of the TKIP (Temporary Key Integrity Protocol). With the TKIP the WEP key is dynamically changed. Herewith, an individual packet coding is realized and the message integrity check is improved.

b) Change or adaption of important system parameters

- Several experiments has been done using a lower radio frequency. The aim is the extension of the possible transmitting range while still exploiting the comparatively cheap COTS products. An additional advantage could be the less interference in the new frequency band. A possible disadvantage may be the reduced available bandwidth. In this case one has to reckon with reduced channel capacity.
- The variation of other important 802.11 parameters with the aim to adapt to specific use is also conceivable. Interesting features for variation could be for example the methods for modulation, spreading or multiplexing. An additional advantage of changed system parameters should be the difficulties for an adversary to use the available 802.11 monitoring or intruding systems without adaptation.

Chapter 9 – NATO REQUIREMENTS MATRIX

Referring to the following documents:

- RTO programme and NATO requirements [18];
- DCI (Defense Capabilities Initiative) document [19];
- LTR 0402 (Advanced Intelligence Network System) [20];
- LTR 2940 (Command & Control C2 – Joint C3I) [21];
- LTR 0430 (Rapid Environmental Assessment) [22]; and
- SACEUR 2030.7/SHPRJ/00 and SACLANT HC-02/Ser NC 0012 (Requirements from the Strategic Command) [24].

We present here in a concise form the NATO requirements and respond with the relevant comments as applicable in the context of the wireless technologies discussed in this document.

9.1 COMMAND AND CONTROL: DEPLOYABILITY OF COMMAND, CONTROL, COMMUNICATIONS AND INFORMATION SYSTEMS (C3I) – FLEXIBILITY OF MOBILE FORCES

The technologies described have as prime goal to serve deployability by ensuring the desired communication possibilities in a rapid, flexible and robust way. The ad-hoc features emphasized in this report serve not only the initial setup but also subsequent movement scenarios for forces and command posts.

Main contributions come from:

- Ad-hoc networking;
- Handover inside the same (military) WPAN/WLAN system; and
- Vertical handover between of different kinds of military WPAN/WLAN systems and cellular networks-civilian or military/public authorities.

The last point refers in particular in urban warfare and antiterrorist operations.

Moreover urban operations need additionally:

- Penetrability of the basic radio technologies for operation inside buildings and/or underground (e.g. UWB as discussed);
- Low frequency bands and narrow bandwidth; and/or
- Setting up relaying mechanisms in a very rapid manner (meshed networking and/or handover techniques).

International standards as described will enable connectivity of equipment from different NATO countries.

9.2 COMMAND & CONTROL: RAPID ENVIRONMENTAL ASSESSMENT (e.g.: FOR WARRIORS)

Sensors and sensor networks serving dismounted soldiers are considered as primary equipment to be served by military. The salient characteristics are:

1) Very low power devices and very short distances (UWB and Bluetooth) as part of a PAN (Personal Area Networks) of an individual warrior; and
2) Low power density communication and larger distances for extended sensor networks.

Security considerations and ESM not important for i. because of extremely short range.

Presenting a unified assessment picture to involved warriors are served by the technologies discussed, in particular via:

1) 802.16 (broadcast, multicast);
2) 802.16 and its mobile extension (for roaming); and
3) 802.11a&b if the same WLAN is moving as a whole (without roaming).

Some drawbacks and hence desirable/necessary improvements, additions and adaptations are:

1) Single point failure of the base station possible (802.16, 802.11 infrastructure mode), whereby ad-hoc routing protocols (e.g. MANET) can enable distribution at application level.
2) Privacy considerations can be presently addressed by encryption enhancements for 802.x (in general) in conjunction with security at higher layers (e.g. IPsec, SSL).
3) Improvement of range is desirable, possibly at the cost of bandwidth by moving to a lower frequency.

For time critical (e.g. firing information) real time assessment is important so that latencies caused mainly by routing updates have to respect stringent bounds. Moreover authentication of the target information source becomes the highest security consideration.

9.3 COMMAND & CONTROL: C2 NETWORK ARCHITECTURES

Ad-hoc routing and wireless technologies provide the main support for flexible network architectures. Contra positioned to this, multiple access techniques displace many of the routing characteristics together with their complexities and problems. By advancing the use of state of the art middleware over such networking infrastructures, a whole new range of applications can be offered down to the last warrior with minimal adaptation effort. This opens also the way to new distributed solutions.

Since all technologies discussed are part of the internet related communication stack, application planning, realization and delivery is greatly facilitated by relying on exclusively internet related developments (three tier architectures for database access, browsers with various plug-ins, etc.).

Increased reliability is achieved by:

1) Flexible routing (a network level feature);
2) Duplication of key functionalities (a middleware level feature); and
3) Provision of location transparency of key networking functions (a network level/management plane feature).

For example routing functionality will be increasingly provided in mobile/low end devices, with minimal infrastructure requirements and at a modest cost.

Wireless (802.11 and 802.16) is expected to replace or to serve as back up to fixed (mainly optically based) interconnection possibilities through ease of installation and reduced costs (as long as bandwidth limitations is not an issue). Approaches of this kind have to be taken into account into any new C2 network architecture design. A concrete and realized case is contained in this report.

9.4 COMMAND & CONTROL: INTEROPERABILITY OF C3I SYSTEMS (ALLIED FORCES / MARITIME, AIR AND LAND OPERATIONS)

9.4.1 Maritime, Air Operations Serving Land Operations

Land operations can initially benefit from an air or ship based command post by employing some of the discussed technologies (e.g. 802.16). Deployability scenarios (as above) can include sea or air based platforms.

Otherwise the discussed wireless technologies do not primarily apply.

9.4.2 Interoperability of Allied Forces

For the benefit of land based operations and the need of common standards, see 9.1 to 9.3.

9.5 COMMAND & CONTROL: CAPACITY OF COMMUNICATION CHANNELS (BANDWIDTH, FREQUENCY SPECTRUM)

The described technologies present an impressive increase in data rates (broadband), and thus open up a whole new range of applications and/or the delivery of existing applications on a much wider and more flexible scale.

This can happen at a relatively low price considering the fact that civilian applications have been the driving force advancing in economic terms the basic technology as well as the available COTS systems and components. This brings also increased need for militarization as each particular application requires. Main additional requirements over and above to what the plain COTS systems can offer concern security improvement, increased range and, low detectability.

Partial military/civilian systems coexistence in the frequency spectrum is a major concern in a several ways:

1) Interoperability with civilian networks, especially in NATO peace keeping operations (positive);
2) Intentional and unintentional interference problems reducing capacity and availability (negative); and
3) Detectability and traffic analysis of wireless traffic pose security risks and open up new terrorist threats.

9.6 COMMAND & CONTROL: SECURITY OF WIRELESS COMMUNICATIONS

Radio and broadcast aspect (monitoring) are the main characteristics differentiating the wireless case from any other fixed and wired environment.

As in other (wired) multiple access systems, **authentication** has to be seen in combination with addressing, low level identification mechanisms and encryption keys (see also additional aspects).

The succession of WEP series of standards improves communication security. In this direction 802.11i deals with dynamic passwords, employs stronger encryption (longer keys) and improved authentication. However management related threats on layer two are poorly covered in the infrastructure node. Denial of service attacks cannot be excluded. Particular protection has to be foreseen to ensure SNMP connections. Additionally the use of secure SNMP should be adopted (rather than the simple versions) to offset the vulnerability of wireless on the physical layer.

Encryption at the lowest layer possible should be the desirable goal, but this would bring new challenges to modify procedures for late entry and actual communication in multiple access systems, beyond that which is nowadays envisaged in the relevant standards. This will conceal headers and will prevent threats based on packet and traffic analysis.

9.7 IMPROVEMENTS OF COMMUNICATIONS AND CONSULTATIONS BETWEEN MILITARY AND CIVIL ORGANIZATIONS (PEACE SUPPORT OPERATIONS)

This calls for a dual approach, i.e. having equipment which is interoperable with civilian systems and in addition contain the enhancements and modifications required to meet military requirements. Hence ideas like software radio could be a long term solution in order to be able to cope with both kinds of waveforms. Handover aspects between different technologies are also crucial.

Another approach is the exploit the ease and flexibility of setting up WLAN islands of restricted radius (even with reduced security characteristics) in combination with ad-hoc networking.

9.8 IMPROVEMENTS IN THE CAPACITY TO OPERATE IN EXTREME WEATHER CONDITIONS (PEACE SUPPORT OPERATIONS)

Mesh structured networks and flexible routing (reducing hop length in case of increased path loss due to precipitation) can solve some of the problems.

Routers have also to be produced in more rugged versions as is customary with more traditional military telecom equipment. The same holds for COTS products (PDAs, Notebooks, antennas, etc.)

9.9 SUSTAINABILITY & LOGISTICS

Enhancement of interoperability through increased standardization and implementation of common communication standards is promoted by the awareness in civilian protocols and relevant products and by identifying their key deficiencies for military use.

9.10 SURVIVABILITY OF FORCES AND INFRASTRUCTURE

This report has reviewed (Chapter 8) the vulnerability of wireless communication and information systems (identification of deficiencies in their resistance to interference and unauthorised access). It has also given some directions to most immediate needs.

Chapter 10 – RECOMMENDATIONS

It is likely that the IEEE 802 standards will be used in military communications systems. They have therefore been thoroughly defined in this report. However, this is a standard in rapid development and since the main body was written, new exiting parts of this standard have emerged which are likely to have significant impact on military communication. One of these activities is the term Cognitive Radio (CR).

The basic premise of CR is that radios can better use the available spectrum by detecting their environment and adapting accordingly. Regulatory agencies such as the Federal Communications Commission (FCC) require that 802.11a radios detect radar signals and avoid interfering with them. This ability to dodge radar requires a significant amount of CR-type adaptability and it is just the beginning of wireless LAN (WLAN) CR capabilities.

WLAN radios may detect a wide variety of radio environment characteristics. These include traffic statistics and other RF events that are identifiable (such as radar, Bluetooth, microprocessor noise or microwave oven noise). They also include such WLAN side effects as collisions, failed packets, adjacent channel interference and hidden stations and unidentifiable noise sources.

By recording RF events, identifying them when possible and responding appropriately, the WLAN radio improves its ability to optimise throughput. Given the amount of interference that can exist in the unlicensed WLAN bands, the radio's CR capabilities are crucial for achieving the robust performance that users expect.

The IEEE will begin work in November 2004 on a standard for fixed-access systems that would use so-called cognitive radio techniques to tap unused swaths of spectrum. The effort, building on the Federal Communications Commission's proposal to open up 300 MHz of unused UHF/VHF spectrum, marks a milestone for software-defined radio (SDR).

These frequency bands are today mainly used for analogue TV broadcasting and military systems. As analogue TV is converted to digital TV (DTV), unused slots become available since DTV uses less spectrum that analogue systems. These frequencies are associated with little path loss and simple technology (CMOS and SDR) and are those, which could make a system cheap to deploy! They are ideally suited for command post inter communications where vehicles are up to a kilometre apart and there is a need to communicate while on the move with LAN rates up to 1 Mbit/s.

The IEEE 802.22 working group is expected to define the media-access control and physical-layer specs for a cognitive air interface that would enable fixed, point-to-multipoint systems working in unused TV spectrum between 54 and 862 MHz to sense and tap available spectrum in that space. This is ideal spectrum for deploying regional networks in sparsely populated areas In that application, 802.22 nets, which could propagate signals up to 40 kilometres, would be rural complements to 802.11 local networks and 802.16 metropolitan backhaul links.

Chapter 11 – REFERENCES

[1] RTO programme and NATO requirements – RTA/SPD (2002-03) PG2002 (NATO UNCLASSIFIED).

[2] Scott Corson, Vincent Park, "Temporally-Ordered Routing Algorithm (TORA) Functional Specification".

[3] D. Johnson, Dave Maltz, Josh Broch, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks".

[4] C Perkins, Elizabeth Royer, "Ad Hoc on Demand Distance Vector (AODV) Routing".

[5] Amir Qayyum, Philippe Jacquet, Paul Muhlethaler, "Optimized Link State Routing Protocol".

[6] Zygmunt Haas, Marc Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks".

[7] Mingliang Jiang, Jinyang Li, Yong Chiang Tay, "Cluster Based Routing Protocol (CBRP) Functional Specification".

[8] Raghupathy Sivakumar, Prasun Sinha, Vaduvur Bharghavan, "Core Extraction Distributed Ad hoc Routing (CEDAR) Specification".

[9] Scott Corson, MANET Routing Protocol Applicability Statement".

[10] Y.C. Tay, C.-K. Toh, C.W. Wu, "Ad hoc Multicast Routing protocol utilizing Increasing id-numberS (AMRIS) Functional Specification".

[11] C Perkins, "Mobile Ad Hoc Networking Terminology".

[12] C-K Toh, "Long-lived Ad Hoc Routing based on the Concept of Associativity".

[13] Evaluation des algorithmes de routage sous le modèle du graphe aléatoire – Philippe Jacquet – Projet Hipercom – INRIA Rocquencourt.

[14] Performance analysis of OLSR Multipoint Relay flooding in two ad hoc wireless network models N°4260 – INRIA Rocquencourt.

[15] AODV Routing Protocol – http://moment.cs.ucsb.edu/AODV/aodv.html

[16] Simulation Results of the OLSR Routing Protocol for Wireless Network – Anis Laouti, Paul Mühlethaler, Abdellah Najid, Epiphane Plakoo – N°4414 – INRIA Rocquencourt.

[17] Optimized Link State Routing Protocol – Draft IETF MANET OLSR 07 – 07/2002 – INRIA Rocquencourt.

[18] RTO programme and NATO requirements – RTA/SPD (2002-03) PG2002 (NATO UNCLASSIFIED).

[19] DCI (Defense Capabilities Initiative) document – PO(99)25 du 15 avril 1999 (NATO CONFIDENTIAL).

[20] LTR (Long Term Requirement in NATO force planning process) 0402 (Advanced Intelligence Network System).

[21] LTR (Long Term Requirement in NATO force planning process) 2940 (Command & Control C2 – Joint C3I).

[22] LTR (Long Term Requirement in NATO force planning process) 0430 (Rapid Environmental Assessment).

[23] SACEUR 2030.7/SHPRJ/00 and SACLANT HC-02/Ser NC 0012 du 25 avril 2000 (Bi-SC guidance for Defense Planning) (NATO CONFIDENTIAL).

[24] IST-035/RTG-015 – Programme of Work/Technical Activities – 24 September 2001.

Annex A – THE PHY AND MAC LAYERS OF 802.16-2001

PHY CONSIDERATIONS

- Line of Sight (because of 10 – 66 GHz)
  - Negligible multi-path => Large channels Large
- Broadband Channels
  - Wide channels (20, 25, or 28 MHz)
  - High capacity – Downlink AND Uplink
- Multiple Access
  - TDM/TDMA
  - High rate burst modems
- Adaptive Burst Profiles on Uplink and Downlink (choose QPSK, 16 QAM, 64 QAM depending on link conditions)
- Multiple duplex schemes
  - Time-Division Duplex (TDD)
  - Frequency-Division Duplex (Frequency-Division Duplex (FDD) [including Burst FDD]
  - Support for Half-Duplex Terminals

ADAPTIVE BURST PROFILES

- Burst profile
  - Modulation and FEC
- Dynamically assigned according to link conditions
  - Burst by burst, per subscriber station
  - Trade-off capacity vs. robustness in real time
- Roughly doubled capacity for the same cell area
- Burst profile for downlink broadcast channel is well-known and robust
  - Other burst profiles can be configured “on the fly”
  - SS capabilities recognized at registration

MODULATION

- Single Carrier QAM, Gray coded
  - QPSK
  - 16QAM

        - Mandatory for Downlink, Optional for Uplink
    - 64QAM
        - Optional for both Downlink and Uplink

- Preambles based on 16-symbol CAZAC sequences

FEC

- Reed Solomon
    - RS GF(256), t =0 …16

- For most critical communications, RS is concatenated with a BCC
    - No interleaving, suitable for burst
    - BCC is a rate 2/3 block code based on a tail-bite termination of the $(7,5)_8$ Convolutional Code for every 16 data bits
    - Shortening allowed

- Turbo Product Codes (TPC) are optional

DUPLEX SCHEME SUPPORT

- On DL, SS addressed in TDM stream

- On UL, SS is allotted a variable length time slot for transmission

- Time-Division Duplex (TDD)
    - DL and UL time-share the same RF channel
    - Dynamic asymmetry
    - SS does not transmit/receive simultaneously (low cost)

- Frequency-Division Duplex (FDD)
    - Downlink and Uplink on separate RF channels
    - Static asymmetry
    - Half-duplex SSs supported
        - SS does not transmit/receive simultaneously (low cost)

BAUD RATES AND CHANNEL SIZE (10 – 66 GHZ)

- Flexible plan – allows equipment manufactures to choose according to spectrum requirements

Channel Width (MHz)	Symbol Rate (Msym/s)	QPSK	16-QAM	64-QAM
		Bit Rate (Mbit/s)	Bit Rate (Mbit/s)	Bit Rate (Mbit/s)
20	16	32	64	96
25	20	40	80	120
28	22.4	44.8	89.6	134.4

802.16 MAC: OVERVIEW

- Point-to-Multipoint
- Metropolitan Area Network
- Connection-oriented
- Supports difficult user environments
  - Very high bit rates, downlink and uplink
  - Hundreds of users per channel
  - Continuous and burst traffic
  - Very efficient use of spectrum
  - Likelihood of terminal being shared (Base Station may be heavily loaded)
- Protocol-Independent core
  - Convergence layers to ATM, IP, Ethernet, ...
- Balances between stability of contentionless and efficiency of contention-based
- Flexible QoS offerings
  - CBR, rt-VBR, nrt-VBR, BE, with granularity within classes
- Supports multiple 802.16 PHYs
  - Adaptive mod, TDD/FDD; single-carrier, OFDM/OFDMA, etc.
- Security

ATM CONVERGENCE SUBLAYER

- Support for:
  - VP (Virtual Path) switched connections
  - VC (Virtual Channel) switched connections
- Support for end-to-end signaling of dynamically created connections:
  - SVCs SVCs

    - Soft soft PVCs PVCs

- ATM header suppression

- Full QoS support

PACKET CONVERGENCE SUBLAYER

- Initial support for Ethernet, IPv4 and IPv6

- Payload header suppression
    - Generic plus IP-specific

- Full QoS support

- Possible future support for:
    - PPP
    - MPLS

MAC ADDRESSING

- SS has 48-bit IEEE MAC Address

- BS has 48-bit Base Station ID
    - Not a MAC address
    - 24-bit operator indicator

- 16-bit Connection ID (CID)
    - Used in MAC PDUs

DOWNLINK TRANSMISSIONS

- Two kinds of bursts: TDM and TDMA

- All bursts are identified by a DIUC
    - Downlink Interval Usage Code

- TDMA bursts have resync preamble
    - Allows for more flexible scheduling

- Each terminal listens to all bursts at its operational IUC, or at a more robust one, except when told to transmit

- Each burst may contain data for several terminals

- SS must recognize the PDUs with known CIDs

- DL-MAP message signals downlink usage

UPLINK TRANSMISSIONS

- Invited transmissions
- Transmissions in contention slots
  - Bandwidth requests
  - Contention resolved using truncated exponential backoff
- Transmissions in initial ranging slots
  - Ranging Requests (RNG-REQ)
  - Contention resolved using truncated exponential backoff
- Bursts defined by UIUCs
- Transmissions allocated by the UL-MAP message
- All transmissions have synchronization preamble
- Ideally, all data from a single SS is concatenated into a single PHY burst

CLASSES OF UPLINK SERVICE

Characteristic of the Service Flow

- Unsolicited Grant Services (UGS)
  - For constant bit-rate (CBR) or CBR-like service flows (SFs) such as T1/E1
- Real-time Polling Services (rtPS)
  - For rt-VBR-like SFs such as MPEG video
- Non-real-time Polling Services (nrtPS)
  - For nrt SFs with better than best effort service such as bandwidth-intensive file transfer
- Best Effort (BE)
  - For best-effort traffic

Annex B – COMMERCIAL PRODUCTS

Find below a non-exhaustive list and short description of a few commercial systems that claim partial compliance with 802.16, or have plans to migrate to become compliant in the future.

WESTERN MULTIPLEX TSUNAMI MULTIPOINT

Tsunami Multipoint offers up to 60 Mbps per base station, and up to six base stations per hub site (or 360 Mbps total capacity). The system scales to support more than 6,000 subscriber units per hub site over an eight mile (13 kilometer) radius.

The new Western Multiplex[1] Tsunami multipoint system[2] features include:

- 360 Mbps Time Division Duplex throughput per cell site for maximum capacity.
- More than 6,000 subscribers per cell site for scalable growth.
- 5.8 GHz frequency band operation.
- Audible beeper alignment and auto-configuration for simple installation.
- Interference rejection option for optimal service reliability.
- Near LOS (line of sight) for maximum service coverage.
- Tsunami Multipoint functionally complies with the emerging IEEE 802.16 standard for broadband wireless access.

MOTOROLA CANOPY

The Motorola Canopy system features are[3]:

- Bandwidth: The system bit rate is 10 Mbps. The measurable throughput is a 7.5 Mbps point-to-point, 6.2 Mbps point-to-multipoint.
- Latency Control: support QoS VoIP, delivers consistent packet latency of 20 ms, regardless of loading.
- Range: The point-to-multipoint range is 10 miles (16 km) and the point-to-point range is 35 miles (56 km).
- Users per AP: Supports 200 Subscriber Modules per AP and 1200 per 6 sector AP cluster.
- Offers 7 non-overlapping channels of operation (3 at 5.2 GHz and 4 at 5.7 GHz) and uses three non-overlapping channels two times in every AP cluster to support 6 APs.
- Can support two (2) six-sector AP clusters and a 5.7 GHz backhaul at a single physical site.
- Offers Dynamic Bandwidth Control on a per AP or a per user basis.
- GPS Synchronization to reduce interference.

Motorola is planning to make Canopy 802.16 compatible.

[1] Note: On March 26, 2002, Western Multiplex merged with Proxim Inc. to create Proxim Corporation.

[2] http://www.wmux.com/company/news/2001/091001Multipoint.html

[3] http://www.motorola.com/canopy

HARRIS CLEARBURST SYSTEMS

The Harris' ClearBurst family of point-to-multipoint broadband wireless access solutions[4] support wireless data and telephony that works across the frequency spectrum from 2 to 40 GHz.

The wideband ClearBurst MB solutions employ FDD technology and support ATM, IP and Ethernet interfaces to help bring up to 28 Mbps of voice, data and e-commerce to small offices and home offices.

The broadband ClearBurst GB solutions employ TDD technology and support ATM, IP and TDM interfaces to help deliver up to 180 Mbps of voice, high-speed data, video conferencing and high-speed Internet access to medium and large companies.

Harris has a migration plan to make these systems fully 802.16 compatible in the future.

BROADSTORM

The Broadstorm system[5] comprises both wireless base stations and compact customer terminals utilizing Broadstorm's OFDMA (orthogonal frequency division multiple access) airlink technology called CelerFlex. The system architecture is all-IP and is aligned with the 802.16a standard. Broadstorm incorporates OFDMA and TDD (time division duplexing) technologies and can provide fixed, portable, or fully mobile solutions to large numbers of customers – up to 3,000 per base station. Broadstorm system can deliver rates up to 8 Mbps per user and total throughput of 48 Mbps per base station.

DRAGONWAVE

DragonLink[6] outdoor radios interface with the customer's indoor networking equipment using either a DOCSIS, 802.16, DAVIC or Proprietary IF interface. The air interface uses FDD or TDD Duplexing with Co or Cross polarization to maximize frequency reuse. DragonLink operates over the bands from 2.0 – 63.0 GHz adaptable to most licensed band allocations around the world.

RUNCOM 802.16 CHIPSETS, MODEMS AND MAC SOFTWARE MODULES

RN-BS22PM Base Station Module[7]

Runcom's RN-BS22PM offers a cost effective module solution for Base Station modem developers of Broadband Wireless Access (BWA) and MMDS applications. The base station module complies with IEEE 802.16a standards and uses OFDMA technology to leverage broadband wireless communication in both downstream and upstream transmissions.

RN-2234 CPE Modem Chip[8]

Runcom's RN-2234 System-On-a-Chip offers a cost effective solution for Customer Premises Equipment (CPE) manufacturers and Subscriber Unit (SU) modem developers of Broadband Wireless Access/MMDS

[4] http://www.microwave.harris.com/products/clearburst/

[5] http://www.broadstorm.com/index.html

[6] http://www.dragonwaveinc.com/products/dl1.htm

[7] http://www.runcom.com/product_page.asp?info_id=48

[8] http://www.runcom.com/info_page.asp?info_id=44

applications. The modem chip complies with IEEE 802.16a standards and uses OFDMA technology to leverage broadband wireless communication in both downstream and upstream transmissions.

MAC Software modules for 802.16 Standard[9]

The RNBS22MAC SW and the RN-2234MAC SW packages are a set of SW modules that provide the functionality required from an IEEE 802.16 standard compliant base-station hub and subscriber units. The SW package supports the core MAC functions defined by the IEEE 802.16 standard air-interface specification and their extension required to support an OFDM/OFDMA PHY as defined by the evolving 802.16a standard supplement.

RunCom also sells Reference Design for 802.16a.

REDLINE COMMUNICATIONS

Redline Communications[10] is developing an AN50 Wireless Access Node that can be operated in the 5 – 8 GHz LE band. This Redline system is based on the emerging IEEE 802.16a standard with the goal of being completely 802.16a compatible once the standard is finalized. The unit is currently a point-to-point system, but development is under way to convert it to a point-to-multipoint one.

The Access Node 50 (AN-50) is a non-line-of-sight, fixed wireless system utilizing advanced orthogonal frequency division multiplexing (OFDM) technology. The AN-50 is configurable to function as a high-speed point-to-point system, operating at up to 72 Mbps over the air per link with up to 16 links per location. The system operates in the license-exempt UNII band of 5.8 GHz and supports ranges beyond 30 miles. The system also features dynamic adaptive modulation in both the upstream and downstream directions, automatically selecting BPSK, QPSK, 16 or 64 QAM, depending on propagation conditions. The system features several antenna options to address deployment ranges of over 50 km.

[9] http://www.runcom.com/info_page.asp?info_id=148

[10] http://www.redlinecommunications.com/

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	RTO-TR-IST-035 AC/323(IST-035)TP/32	ISBN 978-92-837-0052-4	UNCLASSIFIED/ UNLIMITED

5. Originator

Research and Technology Organisation
North Atlantic Treaty Organisation
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies

7. Presented at/Sponsored by

The Final Report of IST-035/RTG-015 submitted by the members of IST-035/RTG-015 for the RTO Information Systems Technology Panel (IST).

8. Author(s)/Editor(s)	9. Date
Multiple	April 2007

10. Author's/Editor's Address	11. Pages
Multiple	122

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other RTO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Commercial equipment
Communication and radio systems
Communications management
Communications networks
Data processing security
Data transmission
Electronic countermeasures
Interoperability
LAN (Local Area Network)
MANET
Military communication
Models
Protocols
QoS (Quality of Service)
Routing protocol
Scenarios
Secure communication
Standardization
Wireless communications
Wireless networks
WLAN (Wireless Local Area Network)
WPAN (Wireless Personal Area Network)

14. Abstract

The context of the IST-035 Task Group work is centered on a broad categorization of technologies and military application areas, such as: WirelessLAN, WirelessPAN, Ad-hoc Network, Command, Post and Vehicles, Soldier Network, Military Relevance, Interoperability, Urban issues.

The present document presents for each technology architecture, security, QoS, performance and frequency aspects. As a reference document it not only discusses technology, but also positions it in the context of the relevant operational deployment. For that reason, the document will be able to take as a starting point the classification of the operational use of COTS systems, made by the SCI-107 WG.

This document is structured around 9 chapters, referring to: ad-hoc networks focusing on MANET; an overview of WLAN technologies; broadband wireless access technologies and protocols; a general approach of a Personal Area Network; Command post and urban operation; the soldier network; Security, ECM and ESM issues.

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DIFFUSION DES PUBLICATIONS
RTO NON CLASSIFIEES

Les publications de l'AGARD et de la RTO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la RTO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (www.rta.nato.int) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der
Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
DSIGRD2 – Bibliothécaire des ressources du savoir
R et D pour la défense Canada
Ministère de la Défense nationale
305, rue Rideau, 9^{e} étage
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics
Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

ETATS-UNIS
NASA Center for AeroSpace
Information (CASI)
Parkway Center, 7121 Standard Drive
Hanover, MD 21076-1320

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research
General Directorate
Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
P O Box 26
H-1525 Budapest

ISLANDE
Director of Aviation
c/o Flugrad
Reykjavik

ITALIE
Centro di Documentazione
Tecnico-Scientifica della Difesa
Via XX Settembre 123
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralny Ośrodek Naukowej
Informacji Wojskowej
Al. Jerozolimskie 97
00-909 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6, 061353, Bucharest

ROYAUME-UNI
Dstl Knowledge Services
Information Centre
Building 247
Dstl Porton Down
Salisbury
Wiltshire SP4 0JQ

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

NASA Center for AeroSpace
Information (CASI)
Parkway Center, 7121 Standard Drive
Hanover, MD 21076-1320
ETATS-UNIS

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council
Acquisitions, Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications RTO et AGARD figurent dans les journaux suivants :

Scientific and Technical Aerospace Reports (STAR)
STAR peut être consulté en ligne au localisateur de
ressources uniformes (URL) suivant:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR est édité par CASI dans le cadre du programme
NASA d'information scientifique et technique (STI)
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
ETATS-UNIS

Government Reports Announcements & Index (GRA&I)
publié par le National Technical Information Service
Springfield
Virginia 2216
ETATS-UNIS
(accessible également en mode interactif dans la base de
données bibliographiques en ligne du NTIS, et sur CD-ROM)

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DISTRIBUTION OF UNCLASSIFIED RTO PUBLICATIONS

AGARD & RTO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO reports, or just those relating to one or more specific RTO Panels, they may be willing to include you (or your Organisation) in their distribution.

RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of RTO reports as they are published, please visit our website (www.rta.nato.int) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère
B-1140 Bruxelles

CANADA
DRDKIM2
Knowledge Resources Librarian
Defence R&D Canada
Department of National Defence
305 Rideau Street, 9th Floor
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

DENMARK
Danish Acquisition and Logistics
Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der
Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research
General Directorate
Research Directorate
Fakinos Base Camp
S.T.G. 1020
Holargos, Athens

HUNGARY
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
P O Box 26
H-1525 Budapest

ICELAND
Director of Aviation
c/o Flugrad, Reykjavik

ITALY
Centro di Documentazione
Tecnico-Scientifica della Difesa
Via XX Settembre 123
00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralny Ośrodek Naukowej
Informacji Wojskowej
Al. Jerozolimskie 97
00-909 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6, 061353, Bucharest

SPAIN
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Knowledge Services
Information Centre
Building 247
Dstl Porton Down
Salisbury, Wiltshire SP4 0JQ

UNITED STATES
NASA Center for AeroSpace
Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320

SALES AGENCIES

NASA Center for AeroSpace
Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
UNITED STATES

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council
Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of RTO and AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
STAR is available on-line at the following uniform
resource locator:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR is published by CASI for the NASA Scientific
and Technical Information (STI) Program
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
UNITED STATES

Government Reports Announcements & Index (GRA&I)
published by the National Technical Information Service
Springfield
Virginia 2216
UNITED STATES
(also available online in the NTIS Bibliographic
Database or on CD-ROM)

ISBN 978-92-837-0052-4